aws

Guide du développeur

AWS WAF, AWS Firewall Manager, et AWS Shield Advanced

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

AWS WAF, AWS Firewall Manager, et AWS Shield Advanced: Guide du développeur

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

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi les clients, ou d’une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d’Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

Table of Contents

Que sont AWS WAF, AWS Shield Advanced ;, et AWS Firewall Manager ?

Vous pouvez utiliser AWS WAFAWS Shield, et AWS Firewall Manager ensemble pour créer une solution de sécurité complète. AWS WAF est un pare-feu d'applications Web que vous pouvez utiliser pour surveiller les requêtes Web que vos utilisateurs finaux envoient à vos applications et pour contrôler l'accès à votre contenu. Shield Advanced fournit une protection contre les attaques par déni de service distribué (DDoS) visant les AWS ressources, les couches réseau et transport (couches 3 et 4) et la couche application (couche 7). AWS Firewall Manager permet de gérer des protections telles que AWS WAF Shield Advanced sur les comptes et les ressources, même lorsque de nouvelles ressources sont ajoutées.

Rubriques

Qu'est-ce que c'est AWS WAF ?

AWS WAF est un pare-feu d'applications Web qui vous permet de surveiller les requêtes HTTP et HTTPS qui sont transmises aux ressources protégées de votre application Web. Vous pouvez protéger les types de ressources suivants :

- CloudFront Distribution sur Amazon
- API REST Amazon API Gateway
- Application Load Balancer
- AWS AppSync API GraphQL
- Groupe d'utilisateurs Amazon Cognito
- AWS App Runner service
- AWS Instance d'accès vérifié

AWS WAF vous permet de contrôler l'accès à votre contenu. Selon les conditions que vous spécifiez, telles que les adresses IP d'où proviennent les demandes ou les valeurs des chaînes de requête,

votre ressource protégée répond aux demandes soit avec le contenu demandé, soit avec un code d'état HTTP 403 (interdit), soit avec une réponse personnalisée.

Au niveau le plus simple, vous AWS WAF permet de choisir l'un des comportements suivants :

- Autoriser toutes les demandes sauf celles que vous spécifiez : cela est utile lorsque vous souhaitez qu'Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito AWS App Runner AWS ou Verified Access diffusent du contenu pour un site Web public, mais que vous souhaitez également bloquer les demandes des attaquants.
- Bloquer toutes les demandes sauf celles que vous spécifiez : cela est utile lorsque vous souhaitez diffuser du contenu pour un site Web restreint dont les utilisateurs sont facilement identifiables grâce aux propriétés des requêtes Web, telles que les adresses IP qu'ils utilisent pour accéder au site Web.
- Comptez les demandes qui correspondent à vos critères : vous pouvez utiliser cette Count action pour suivre votre trafic Web sans modifier la façon dont vous le gérez. Vous pouvez l'utiliser pour une surveillance générale et également pour tester vos nouvelles règles de gestion des requêtes Web. Lorsque vous souhaitez autoriser ou bloquer des demandes en fonction des nouvelles propriétés des requêtes Web, vous pouvez d'abord configurer AWS WAF pour compter les demandes correspondant à ces propriétés. Cela vous permet de confirmer vos nouveaux paramètres de configuration avant de modifier vos règles pour autoriser ou bloquer les demandes correspondantes.
- Exécutez des CAPTCHA ou des contrôles de contestation en fonction des demandes correspondant à vos critères : vous pouvez mettre en œuvre des CAPTCHA et des contrôles de contestation silencieux pour les demandes afin de réduire le trafic de robots vers vos ressources protégées.

L'utilisation AWS WAF présente plusieurs avantages :

- Protection supplémentaire contre les attaques Web à l'aide de critères que vous spécifiez. Vous pouvez définir des critères à l'aide des caractéristiques des requêtes Web, telles que les suivantes :
  - Les adresses IP d'où proviennent les requêtes.
  - Pays d'où proviennent les demandes.
  - Les valeurs des en-têtes des requêtes.
  - Chaînes qui apparaissent dans les demandes, qu'il s'agisse de chaînes spécifiques ou de chaînes correspondant à des modèles d'expressions régulières (regex).

  - La longueur des requêtes.
  - La présence de code SQL susceptible d'être malveillant (appelée injection SQL).
  - La présence d'un script susceptible d'être malveillant (appelé script inter-site).
- Règles permettant d'autoriser, de bloquer ou de compter les requêtes Web répondant aux critères spécifiés. Les règles peuvent également bloquer ou compter les requêtes Web qui non seulement répondent aux critères spécifiés, mais dépassent également un certain nombre de demandes en une minute ou en cinq minutes.
- Règles que vous pouvez réutiliser pour plusieurs applications web.
- Groupes de règles gérés par AWS et par AWS Marketplace les vendeurs.
- Métriques en temps réel et exemples de requêtes web.
- Administration automatisée à l'aide de l' AWS WAF API.

Si vous souhaitez contrôler de manière granulaire les protections que vous ajoutez à vos ressources, AWS WAF seule peut être le bon choix. Pour plus d'informations sur AWS WAF, voirAWS WAF.

Qu'est-ce que c'est AWS Shield Advanced ?

Vous pouvez utiliser des listes de contrôle d'accès AWS WAF Web (ACL Web) pour minimiser les effets d'une attaque par déni de service distribué (DDoS). Pour une protection supplémentaire contre les attaques DDoS, fournit AWS également AWS Shield Standard et AWS Shield Advanced. AWS Shield Standard est automatiquement inclus sans frais supplémentaires au-delà de ce que vous avez déjà payé AWS WAF et de vos autres AWS services.

Shield Advanced fournit une protection étendue contre les attaques DDoS pour vos instances Amazon EC2, vos équilibreurs de charge Elastic Load Balancing, vos distributions CloudFront , vos zones hébergées Route 53 et vos accélérateurs standard. AWS Global Accelerator Shield Advanced entraîne des frais supplémentaires. Les options et fonctionnalités avancées de Shield incluent l'atténuation automatique des attaques DDoS au niveau de l'application, une visibilité avancée des événements et le support dédié de la Shield Response Team (SRT). Si vous possédez des sites Web très visibles ou si vous êtes exposé à de fréquentes attaques DDoS, pensez à acheter les protections supplémentaires fournies par Shield Advanced. Pour en savoir plus, consultez AWS Shield Advanced capacités et options et Décider s'il convient de souscrire à des protections supplémentaires AWS Shield Advanced et d'appliquer des protections supplémentaires.

Qu'est-ce que c'est AWS Firewall Manager ?

AWS Firewall Manager simplifie vos tâches d'administration et de maintenance sur plusieurs comptes et ressources pour diverses protections AWS WAF AWS Shield Advanced, notamment les groupes de sécurité Amazon VPC et les ACL réseau, AWS Network Firewall ainsi que le pare-feu DNS Amazon Route 53 Resolver. Avec Firewall Manager, vous configurez vos protections une seule fois et le service les applique automatiquement à tous vos comptes et ressources, même lorsque vous ajoutez de nouveaux comptes et ressources.

Pour en savoir plus sur Firewall Manager, consultez AWS Firewall Manager.

Configuration de votre compte pour utiliser les services

Cette rubrique décrit les étapes préliminaires, telles que la création d'un compte, pour vous préparer à utiliser AWS WAF AWS Firewall Manager, et AWS Shield Advanced. Ces articles préliminaires ne vous sont pas facturés. Seuls les AWS services que vous utilisez vous sont facturés.

Rubriques

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.
2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

   Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Télécharger les outils

AWS Management Console Il inclut une console pour AWS WAF, et AWS Shield Advanced AWS Firewall Manager, mais si vous souhaitez accéder aux services par programmation, consultez ce qui suit :

- Les guides d'API documentent les opérations prises en charge par les services et fournissent des liens vers la documentation relative au SDK et à la CLI :
  - AWS WAF API Reference
  - AWS Shield Advanced API Reference
  - AWS Firewall Manager API Reference
- Pour appeler une API sans avoir à gérer des détails de bas niveau tels que l'assemblage de requêtes HTTP brutes, vous pouvez utiliser un AWS SDK. Les AWS SDK fournissent des fonctions et des types de données qui encapsulent les fonctionnalités des AWS services. Pour télécharger un AWS SDK et accéder aux instructions d'installation, consultez la page correspondante :
  - Java
  - JavaScript
  - .NET

- Node.js
- PHP
- Python
- Ruby

Pour obtenir la liste complète des AWS SDK, consultez la section Outils pour Amazon Web Services.

- Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour contrôler plusieurs AWS services à partir de la ligne de commande. Vous pouvez également automatiser vos commandes à l'aide de scripts. Pour plus d’informations, consultez AWS Command Line Interface.
- AWS Tools for Windows PowerShell soutient ces AWS services. Pour plus d'informations, consultez le Guide de référence des cmdlets AWS Tools for PowerShell.

AWS WAF

AWS WAF est un pare-feu d'applications Web qui vous permet de surveiller les requêtes HTTP (S) qui sont transmises aux ressources protégées de votre application Web. Vous pouvez protéger les types de ressources suivants :

- CloudFront Distribution sur Amazon
- API REST d'Amazon API Gateway
- Application Load Balancer
- AWS AppSync API GraphQL
- Groupe d'utilisateurs Amazon Cognito
- AWS App Runner service
- AWS Instance d'accès vérifié

AWS WAF vous permet de contrôler l'accès à votre contenu. Sur la base de critères que vous spécifiez, tels que les adresses IP d'où proviennent les demandes ou les valeurs des chaînes de requête, le service associé à votre ressource protégée répond aux demandes soit avec le contenu demandé, soit avec un code d'état HTTP 403 (Interdit), soit avec une réponse personnalisée.

> **Note**
>
> Vous pouvez également l'utiliser AWS WAF pour protéger vos applications hébergées dans des conteneurs Amazon Elastic Container Service (Amazon ECS). Amazon ECS est un service de gestion de conteneurs rapide et hautement évolutif qui facilite l'exécution, l'arrêt et la gestion des conteneurs Docker sur un cluster. Pour utiliser cette option, vous configurez Amazon ECS de manière à utiliser un Application Load Balancer activé AWS WAF pour acheminer et protéger le trafic HTTP (S) de couche 7 entre les tâches de votre service. Pour plus d'informations, consultez la section Service Load Balancing dans le manuel Amazon Elastic Container Service Developer Guide.

Rubriques

- AWS WAF groupes de règles
- AWS WAF règles
- Gestion des composants de demande surdimensionnés dans AWS WAF
- Modèle d'expression régulière correspondant dans AWS WAF
- Ensembles d'adresses IP et ensembles de modèles regex dans AWS WAF
- Demandes et réponses Web personnalisées dans AWS WAF
- AWS WAF étiquettes sur les requêtes Web
- AWS WAF Atténuation intelligente des menaces
- Journalisation AWS WAF du trafic ACL Web
- Tester et ajuster vos AWS WAF protections
- Comment AWS WAF fonctionne avec les CloudFront fonctionnalités d'Amazon
- Sécurité lors de votre utilisation du AWS WAF service
- AWS WAF quotas
- Migration de vos ressources AWS WAF classiques vers AWS WAF

Comment AWS WAF fonctionne

Vous pouvez AWS WAF contrôler la façon dont vos ressources protégées répondent aux requêtes Web HTTP (S). Pour ce faire, définissez une liste de contrôle d'accès Web (ACL), puis associez-la à une ou plusieurs ressources d'applications Web que vous souhaitez protéger. Les ressources associées transmettent les demandes entrantes à l'ACL Web AWS WAF pour inspection.

Dans votre ACL Web, vous créez des règles pour définir les modèles de trafic à rechercher dans les demandes et pour spécifier les actions à effectuer pour les demandes correspondantes. Les options d'action sont les suivantes :

- Autorisez les demandes à accéder à la ressource protégée pour traitement et réponse.
- Bloquez les demandes.
- Comptez les demandes.
- Exécutez des CAPTCHA ou des contrôles par rapport aux demandes afin de vérifier l'utilisation standard du navigateur par les utilisateurs humains.

AWS WAF composants

Voici les principaux éléments de AWS WAF :

- ACL Web : vous utilisez une liste de contrôle d'accès Web (ACL) pour protéger un ensemble de AWS ressources. Vous créez une liste ACL Web et définissez sa stratégie de protection en ajoutant des règles. Les règles définissent les critères d'inspection des requêtes Web et spécifient les mesures à prendre pour les demandes correspondant à ces critères. Vous définissez également une action par défaut pour l'ACL Web qui indique s'il faut bloquer ou autoriser les demandes que les règles n'ont pas déjà bloquées ou autorisées. Pour en savoir plus sur les listes ACL, veuillez consulter AWS WAF listes de contrôle d'accès Web (ACL Web).

  Une ACL Web est une AWS WAF ressource.

- Règles : chaque règle contient une déclaration qui définit les critères d'inspection et une action à entreprendre si une requête Web répond aux critères. Lorsqu'une demande Web répond aux critères, c'est une correspondance. Vous pouvez configurer des règles pour bloquer les demandes correspondantes, les autoriser à passer, les compter ou exécuter des contrôles par bot à l'aide de puzzles CAPTCHA ou de défis de navigateur client silencieux. Pour plus d'informations sur les règles, consultez AWS WAF règles.

  Une règle n'est pas une AWS WAF ressource. Il n'existe que dans le contexte d'une ACL Web ou d'un groupe de règles.

- Groupes de règles : vous pouvez définir des règles directement dans une ACL Web ou dans des groupes de règles réutilisables. AWS Règles gérées et AWS Marketplace les vendeurs mettent à votre disposition des groupes de règles gérés. Vous pouvez également définir vos propres groupes de règles. Pour de plus amples informations sur les groupes de correctifs, veuillez consulter AWS WAF groupes de règles.

  Un groupe de règles est une AWS WAF ressource.

Rubriques

AWS WAF unités de capacité ACL Web (WCU)

AWS WAF utilise les unités de capacité ACL (WCU) Web pour calculer et contrôler les ressources d'exploitation nécessaires à l'exécution de vos règles, groupes de règles et ACL Web. AWS WAF

applique les limites de la WCU lorsque vous configurez vos groupes de règles et vos ACL Web. Les WCU n'affectent pas la façon dont le trafic Web AWS WAF est inspecté.

AWS WAF gère la capacité des règles, des groupes de règles et des ACL Web.

Règle WCU

AWS WAF calcule la capacité des règles lorsque vous créez ou mettez à jour une règle. AWS WAF calcule la capacité différemment pour chaque type de règle, afin de refléter le coût relatif de chaque règle. Les règles simples qui coûtent peu d'exécution utilisent moins de WCU que les règles plus complexes qui utilisent plus de puissance de traitement. Par exemple, une instruction de règle de contrainte de taille utilise moins de WCU qu'une instruction qui inspecte les demandes à l'aide d'un ensemble de modèles regex.

Les exigences en matière de capacité des règles commencent généralement par un coût de base pour le type de règle et augmentent avec la complexité, par exemple, lorsque vous ajoutez des transformations de texte avant l'inspection ou si vous inspectez le corps du fichier JSON. Pour plus d'informations sur les exigences de capacité des règles, consultez les listes des instructions de règles à l'adresseNotions de base sur les énoncés.

Groupe de règles WCU

Les exigences WCU pour un groupe de règles sont déterminées par les règles que vous définissez au sein du groupe de règles. La capacité maximale d'un groupe de règles est de 5 000 WCU.

Chaque groupe de règles possède un paramètre de capacité immuable, que le propriétaire attribue lors de sa création. Cela est vrai pour les groupes de règles gérés et les groupes de règles que vous créez via AWS WAF. Lorsque vous modifiez un groupe de règles, vos modifications doivent maintenir les WCU du groupe de règles dans les limites de leurs capacités. Cela garantit que les ACL Web qui utilisent le groupe de règles respectent leurs exigences en matière de capacité.

Les WCU utilisés dans un groupe de règles sont la somme des WCU pour les règles moins les optimisations de traitement pouvant être AWS WAF obtenues en combinant le comportement des règles. Par exemple, si vous définissez deux règles pour examiner le même composant de requête Web et que les règles appliquent chacune une transformation particulière au composant avant de l'inspecter, vous pourrez AWS WAF peut-être vous facturer une seule fois pour l'application de la transformation. Le coût WCU lié à l'utilisation d'un groupe de règles dans une ACL Web est toujours le paramètre WCU fixe que vous avez défini lors de la création du groupe de règles.

Lorsque vous créez un groupe de règles, veillez à définir une capacité suffisamment élevée pour tenir compte des règles que vous souhaiterez utiliser pendant toute la durée de vie du groupe de règles.

WCU ACL Web

Les exigences WCU pour une ACL Web sont déterminées par les règles et les groupes de règles que vous utilisez dans l'ACL Web.

- Le coût d'utilisation d'un groupe de règles dans une ACL Web est le paramètre de capacité du groupe de règles.
- Le coût d'utilisation d'une règle est le WCU calculé par la règle moins les optimisations de traitement pouvant être obtenues à partir de la combinaison de règles de l'ACL Web. AWS WAF Par exemple, si vous définissez deux règles pour examiner le même composant de requête Web et que les règles appliquent chacune une transformation particulière au composant avant de l'inspecter, vous pourrez AWS WAF peut-être vous facturer une seule fois pour l'application de la transformation.

Le prix de base d'une ACL Web comprend jusqu'à 1 500 WCU. L'utilisation de plus de 1 500 WCU entraîne des frais supplémentaires, selon un modèle de tarification à plusieurs niveaux. AWS WAF ajuste automatiquement la tarification de votre ACL Web en fonction de l'évolution de l'utilisation de votre WCU ACL Web. Pour plus d'informations sur la tarification, consultez la page AWS WAF Pricing (Tarification).

La capacité maximale d'une ACL Web est de 5 000 WCU.

Déterminer les WCU pour un groupe de règles ou une ACL Web

Comme indiqué dans les sections précédentes, le total des WCU utilisés dans un groupe de règles ou une ACL Web sera égal ou inférieur à la somme des WCU pour toutes les règles définies dans le groupe de règles ou l'ACL Web.

Dans la AWS WAF console, vous pouvez voir la capacité consommée lorsque vous ajoutez des règles à votre ACL Web ou à votre groupe de règles. La console affiche les unités de capacité actuellement utilisées lorsque vous ajoutez les règles.

Grâce à l'API, vous pouvez vérifier les exigences de capacité maximale pour les règles que vous souhaitez utiliser dans une ACL Web ou un groupe de règles. Pour ce faire, fournissez la liste JSON des règles à l'appel de vérification de capacité. Pour plus d'informations, consultez CheckCapacityla référence de l'API AWS WAF V2.

Des ressources que vous pouvez protéger AWS WAF

Vous pouvez utiliser une ACL AWS WAF Web pour protéger les types de ressources mondiaux ou régionaux. Pour ce faire, associez l'ACL Web aux ressources que vous souhaitez protéger. L'ACL Web et toutes AWS WAF les ressources qu'il utilise doivent se trouver dans la région où se trouve la ressource associée. Pour les CloudFront distributions Amazon, cette option est définie sur USA Est (Virginie du Nord).

CloudFront Distributions Amazon

Vous pouvez associer une ACL AWS WAF Web à une CloudFront distribution à l'aide de la AWS WAF console ou des API. Vous pouvez également associer une ACL Web à une CloudFront distribution lorsque vous créez ou mettez à jour la distribution elle-même. Pour configurer une association dans AWS CloudFormation, vous devez utiliser la configuration CloudFront de distribution. Pour plus d'informations sur Amazon CloudFront, consultez la section Utiliser AWS WAF pour contrôler l'accès à votre contenu dans le manuel Amazon CloudFront Developer Guide.

AWS WAF est disponible dans le monde entier pour les CloudFront distributions, mais vous devez utiliser la région USA Est (Virginie du Nord) pour créer votre ACL Web et toutes les ressources utilisées dans l'ACL Web, telles que les groupes de règles, les ensembles d'adresses IP et les ensembles de modèles regex. Certaines interfaces proposent le choix de région « Global (CloudFront) ». Le choix de cette option est identique à celui de la région USA Est (Virginie du Nord) ou « us-east-1 ».

Ressources régionales

Vous pouvez protéger les ressources régionales dans toutes les régions où AWS WAF elles sont disponibles. Vous pouvez consulter la liste des AWS WAF points de terminaison et des quotas dans le Référence générale d'Amazon Web Services.

Vous pouvez l'utiliser AWS WAF pour protéger les types de ressources régionaux suivants :

- API REST Amazon API Gateway
- Application Load Balancer
- AWS AppSync API GraphQL
- Groupe d'utilisateurs Amazon Cognito
- AWS App Runner service
- AWS Instance d'accès vérifié

Vous ne pouvez associer une ACL Web qu'à un Application Load Balancer qui s'y trouve. Régions AWS Par exemple, vous ne pouvez pas associer une ACL Web à un Application Load Balancer activé. AWS Outposts

L'ACL Web et toutes AWS WAF les autres ressources qu'il utilise doivent être situées dans la même région que les ressources protégées. Lors de la surveillance et de la gestion des requêtes Web pour une ressource régionale protégée, AWS WAF conserve toutes les données dans la même région que la ressource protégée.

Restrictions relatives aux associations de ressources multiples

Vous pouvez associer une seule ACL Web à une ou plusieurs AWS ressources, avec les restrictions suivantes :

- Vous ne pouvez associer chaque AWS ressource qu'à une seule ACL Web. La relation entre l'ACL Web et AWS les ressources est one-to-many.
- Vous pouvez associer une ACL Web à une ou plusieurs CloudFront distributions. Vous ne pouvez associer une ACL Web que vous avez associée à une CloudFront distribution à aucun autre type de AWS ressource.

Commencer avec AWS WAF

Ce didacticiel montre comment AWS WAF effectuer les tâches suivantes :

- Configurez AWS WAF.
- Créez une liste de contrôle d'accès Web (ACL Web) à l'aide de l'assistant de la AWS WAF console.
- Choisissez les AWS ressources pour lesquelles vous AWS WAF souhaitez inspecter les requêtes Web. Ce didacticiel décrit les étapes à suivre pour Amazon CloudFront. Le processus est essentiellement le même pour une API REST Amazon API Gateway, un Application Load Balancer, une API AWS AppSync GraphQL, un groupe d'utilisateurs Amazon Cognito, un AWS App Runner service ou une instance Verified Access. AWS
- Ajoutez les règles et les groupes de règles que vous souhaitez utiliser pour filtrer les demandes web. Par exemple, vous pouvez spécifier les adresses IP d'où proviennent les demandes et spécifier des valeurs dans la demande qui ne sont utilisées que par les attaquants. Pour chaque règle, vous spécifiez comment traiter les requêtes Web correspondantes. Vous pouvez faire des choses comme les bloquer ou les compter et vous pouvez lancer des défis de bot tels que

CAPTCHA. Vous définissez une action pour chaque règle que vous définissez dans une ACL Web et pour chaque règle que vous définissez dans un groupe de règles.

- Spécifiez une action par défaut pour l'ACL Web, Block soitAllow. Il s'agit de l'action qui AWS WAF exécute une demande lorsque les règles de l'ACL Web ne l'autorisent ou ne la bloquent pas explicitement.

> **Note**
>
> AWS vous facture généralement moins de 0,25 USD par jour pour les ressources que vous créez au cours de ce didacticiel. Lorsque vous avez terminé les opérations dans le cadre de ce didacticiel, nous vous recommandons de supprimer les ressources pour éviter de générer des frais supplémentaires.

Rubriques

Étape 1 : Configuration AWS WAF

Si vous n'avez pas encore suivi les étapes générales de configurationConfiguration de votre compte pour utiliser les services, faites-le maintenant.

Étape 2 : Créer une liste ACL web

La AWS WAF console vous guide tout au long du processus de configuration AWS WAF pour bloquer ou autoriser les requêtes Web en fonction de critères que vous spécifiez, tels que les adresses IP d'où proviennent les demandes ou les valeurs contenues dans les demandes. Au cours de cette étape, vous créez une liste ACL Web. Pour plus d'informations sur les ACL AWS WAF Web, consultezAWS WAF listes de contrôle d'accès Web (ACL Web).

Pour créer une liste ACL web

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Sur la page d' AWS WAF accueil, choisissez Create web ACL.
3. Dans Nom (Nom), entrez le nom que vous souhaitez utiliser pour identifier cette liste ACL web.

   > **Note**
   >
   > Vous ne pouvez pas modifier le nom une fois que vous créez la liste ACL web.

4. (Facultatif) Pour Description - facultatif, entrez une description plus longue pour la liste ACL web si vous le souhaitez.
5. Pour le nom de la CloudWatch métrique, modifiez le nom par défaut le cas échéant. Suivez les instructions sur la console pour connaître les caractères valides. Le nom ne peut pas contenir de caractères spéciaux, d'espaces blancs ou de noms de métriques réservés pour AWS WAF, y compris « All » et « Default_Action ». «

   > **Note**
   >
   > Vous ne pouvez pas modifier le nom de la CloudWatch métrique après avoir créé l'ACL Web.

6. Pour Type de ressource, choisissez CloudFrontles distributions. La région est automatiquement renseignée en Global (CloudFront) pour les CloudFront distributions.
7. (Facultatif) Pour AWS Ressources associées : facultatif, choisissez Ajouter AWS des ressources. Dans la boîte de dialogue, choisissez les ressources que vous souhaitez associer, puis cliquez sur Ajouter. AWS WAF vous renvoie à la page Describe Web ACL et aux AWS ressources associées.
8. Choisissez Suivant.

Étape 3 : Ajouter une règle de correspondance de chaîne

Dans cette étape, vous créez une règle avec une instruction de correspondance de chaîne et indiquez ce qu'il faut faire avec les demandes de correspondance. Une instruction de règle de correspondance de chaînes identifie les chaînes que vous AWS WAF souhaitez rechercher dans une demande. Généralement, une chaîne est composée de caractères ASCII imprimables, mais

vous pouvez spécifier n'importe quel caractère de valeur hexadécimale 0x00 à 0xFF (de valeur décimale 0 à 255). Outre la chaîne à rechercher, vous spécifiez le composant de requête Web que vous souhaitez rechercher, tel qu'un en-tête, une chaîne de requête ou le corps de la demande.

Ce type d'instruction fonctionne sur un composant de requête Web et nécessite les paramètres de composant de demande suivants :

- Composant de demande : partie de la requête Web destinée à inspecter, par exemple, une chaîne de requête ou le corps de la requête.

  > **Warning**
  >
  > Si vous inspectez les composants de la requête Body, JSON body, Headers ou Cookies, renseignez-vous sur les limites relatives à Gestion des composants de demande surdimensionnés dans AWS WAF la quantité de contenu AWS WAF pouvant être inspectée.

  Pour plus d'informations sur les composants des requêtes Web, consultezSpécification et gestion des composants de requête Web.
- Transformations de texte facultatives : transformations que vous AWS WAF souhaitez effectuer sur le composant de demande avant de l'inspecter. Par exemple, vous pouvez passer en minuscules ou normaliser les espaces blancs. Si vous spécifiez plusieurs transformations, AWS WAF traitez-les dans l'ordre indiqué. Pour plus d'informations, consultez Options de transformation du texte.

Pour plus d'informations sur AWS WAF les règles, consultezAWS WAF règles.

Pour créer une instruction de règle de correspondance de chaîne

1. Sur la page Ajouter des règles et des groupes de règles, choisissez Ajouter des règles, Ajouter mes propres règles et groupes de règles, Générateur de règles, puis Éditeur visuel de règles.

   > **Note**
   >
   > La console fournit l' éditeur visuel de règles ainsi qu'un éditeur JSON de règles. L'éditeur JSON vous permet de copier facilement des configurations entre les listes ACL web et est requis pour les jeux de règles plus complexes, comme ceux avec plusieurs niveaux d'imbrication.

Cette procédure utilise l' éditeur visuel de règles.

2. Dans la zone Nom, entrez le nom que vous souhaitez utiliser pour identifier cette règle.
3. Pour Type choisissez Règle régulière.
4. Pour Si une demande choisissez correspond à l'instruction.

   Les autres options concernent les types d'instructions de règles logiques. Vous pouvez les utiliser pour combiner ou annuler les résultats d'autres déclarations de règles.
5. Dans Statement, pour Inspect, ouvrez le menu déroulant et choisissez le composant de requête Web que vous AWS WAF souhaitez inspecter. Pour cet exemple, choisissez Header.

   Lorsque vous choisissez En-tête, vous spécifiez également l'en-tête que AWS WAF doit inspecter. Saisissez **`User-Agent`**. Cette valeur n'est pas sensible à la casse.
6. Pour Type de correspondance, choisissez l'endroit où la chaîne spécifiée doit apparaître dans l'en-tête `User-Agent`.

   Pour cet exemple, choisissez Exactly matches string (Correspond exactement à la chaîne). Cela indique qu'il AWS WAF inspecte l'en-tête de l'agent utilisateur dans chaque requête Web pour détecter une chaîne identique à la chaîne que vous spécifiez.
7. Pour que String to match (Chaîne de correspondance), spécifiez la chaîne que AWS WAF doit rechercher. La longueur maximale de String to match (Chaîne de correspondance) est 200 caractères. Si vous souhaitez spécifier une valeur codée en base64, vous pouvez spécifier jusqu'à 200 caractères avant l'encodage.

   Pour cet exemple, entrez MyAgent. AWS WAF inspectera la valeur de l'`User-Agent`en-tête dans les requêtes Web`MyAgent`.
8. Laissez Text transformation (Transformation de texte) définie sur None (Aucun).
9. Pour Action, sélectionnez l'action que vous souhaitez que la règle exécute lorsqu'elle correspond à une requête Web. Pour cet exemple, choisissez Count et laissez les autres choix tels quels. L'action de comptage crée des métriques pour les requêtes Web conformes à la règle, mais n'a aucune incidence sur le fait que la demande soit autorisée ou bloquée. Pour plus d'informations sur les choix d'action, reportez-vous Action de la règle aux sections etÉvaluation des règles ACL Web et des groupes de règles.
10. Choisissez Ajouter une règle.

Étape 4 : Ajouter un groupe de règles AWS gérées

AWS Managed Rules propose un ensemble de groupes de règles gérés que vous pouvez utiliser, dont la plupart sont gratuits pour AWS WAF les clients. Pour de plus amples informations sur les groupes de correctifs, veuillez consulter AWS WAF groupes de règles. Nous allons ajouter un groupe de règles AWS gérées à cette ACL Web.

Pour ajouter un groupe de règles AWS gérées

1. Dans la page Ajouter des règles et des groupes de règles, choisissez Ajouter des règles, puis Ajouter des groupes de règles gérées.
2. Dans la page Ajouter des groupes de règles gérées développez la liste des groupes de règles gérées par AWS . (Vous verrez également les offres proposées aux AWS Marketplace vendeurs. Vous pouvez vous abonner à leurs offres, puis les utiliser de la même manière que pour les groupes de règles AWS Managed Rules.)
3. Pour le groupe de règles que vous souhaitez ajouter, procédez comme suit :
    a. Dans la colonne Action, activez le bouton Ajouter à l'ACL Web.
    b. Sélectionnez Modifier et, dans la liste des règles du groupe de règles, ouvrez le menu déroulant Annuler toutes les actions des règles et sélectionnez. Count Cela définit l'action pour que toutes les règles du groupe de règles soient uniquement comptabilisées. Cela vous permet de voir comment toutes les règles du groupe de règles se comportent avec vos requêtes Web avant de les utiliser.
    c. Choisissez Enregistrer la règle.
4. Sur la page Ajouter des groupes de règles gérés, sélectionnez Ajouter des règles. Cela vous renvoie à la page Ajouter des règles et des groupes de règles.

Étape 5 : terminer la configuration de votre ACL Web

Lorsque vous avez terminé d'ajouter des règles et des groupes de règles à votre configuration ACL web, terminez en gérant la priorité des règles dans la liste ACL web et en configurant des paramètres tels que les métriques, le balisage et la journalisation.

Pour terminer la configuration de la liste ACL web

1. Dans la page Ajouter des règles et des groupes de règles, choisissez Suivant.

2. Sur la page Définir la priorité des règles, vous pouvez voir l'ordre de traitement des règles et des groupes de règles dans l'ACL Web. AWS WAF les traite en commençant par le haut de la liste. Vous pouvez modifier l'ordre de traitement en déplaçant les règles vers le haut ou vers le bas. Pour ce faire, sélectionnez-en une dans la liste et choisissez Déplacer vers le haut ou Déplacer vers le bas. Pour plus d'informations sur la priorité des règles, consultez Ordre de traitement des règles et des groupes de règles dans une ACL Web.
3. Choisissez Suivant.
4. Sur la page Configurer les métriques, pour les CloudWatchmétriques Amazon, vous pouvez voir les métriques planifiées pour vos règles et groupes de règles, ainsi que les options d'échantillonnage des requêtes Web. Pour plus d'informations sur l'affichage des exemples de demandes, consultezAffichage d'un exemple de demandes web. Pour plus d'informations sur CloudWatch les métriques Amazon, consultezSurveillance avec Amazon CloudWatch.

   Vous pouvez accéder aux résumés des mesures du trafic Web sur la page de l'ACL Web dans la AWS WAF console, sous l'onglet Aperçu du trafic. Les tableaux de bord de la console fournissent des résumés en temps quasi réel des métriques Amazon CloudWatch de l'ACL Web. Pour plus d'informations, consultez Tableaux de bord de présentation du trafic Web ACL.
5. Choisissez Suivant.
6. Sur la page Vérifier et créer les listes ACL web vérifiez vos paramètres, puis choisissez Créer une liste ACL web.

L'Assistant vous renvoie à la page Listes ACL Web où votre nouvelle ACL web est répertoriée.

Étape 6 : Nettoyer vos ressources

Vous avez maintenant terminé le didacticiel. Pour éviter que votre compte n'entraîne des AWS WAF frais supplémentaires, nettoyez les AWS WAF objets que vous avez créés. Vous pouvez également modifier la configuration pour qu'elle corresponde aux requêtes Web que vous souhaitez réellement gérer à l'aide de celles-ci AWS WAF.

> **Note**
>
> AWS vous facture généralement moins de 0,25 USD par jour pour les ressources que vous créez au cours de ce didacticiel. Lorsque vous avez terminé, nous vous recommandons de supprimer les ressources pour éviter de générer des frais supplémentaires.

Pour supprimer les objets AWS WAF payants

1. Dans la page Liste ACL web sélectionnez votre liste ACL web dans la liste et choisissez Edit (Modifier).
2. Dans l'onglet AWS Ressources associées, pour chaque ressource associée, sélectionnez le bouton radio à côté du nom de la ressource, puis choisissez Dissocier. Cela dissocie l'ACL Web de vos AWS ressources.
3. Dans chacun des écrans suivants, choisissez Suivant jusqu'à ce que vous reveniez à la page Listes ACL web.

   Dans la page Liste ACL web sélectionnez votre ACL web dans la liste et choisissez Supprimer.

Les règles et les instructions de règle n'existent pas en dehors des définitions de groupe de règles et de listes ACL Web. Si vous supprimez une liste ACL Web, toutes les règles individuelles que vous avez définies dans la liste ACL Web sont supprimées. Lorsque vous supprimez un groupe de règles d'une liste ACL Web, vous supprimez simplement la référence à celui-ci.

AWS WAF listes de contrôle d'accès Web (ACL Web)

Une liste de contrôle d'accès Web (ACL Web) vous permet de contrôler avec précision toutes les requêtes Web HTTP (S) auxquelles répond votre ressource protégée. Vous pouvez protéger les ressources Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito AWS et AWS App Runner Verified Access.

Vous pouvez utiliser des critères tels que les suivants pour autoriser ou bloquer les demandes :

- Origine de l'adresse IP de la demande
- Pays d'origine de la demande
- Correspondance de chaîne ou expression régulière (regex) dans une partie de la demande
- Taille d'une partie particulière de la demande
- Détection de code SQL ou scripts malveillants

Vous pouvez également tester n'importe quelle combinaison de ces conditions. Vous pouvez bloquer ou compter les requêtes Web qui non seulement répondent aux conditions spécifiées, mais qui dépassent également un certain nombre de demandes en une minute. Vous pouvez combiner des

conditions à l'aide d'opérateurs logiques. Vous pouvez également exécuter des puzzles CAPTCHA et des défis de session client silencieux en réponse à des demandes.

Vous indiquez vos critères de correspondance et les mesures à prendre en cas de correspondance dans les déclarations de AWS WAF règles. Vous pouvez définir des instructions de règles directement dans votre ACL Web et dans des groupes de règles réutilisables que vous utilisez dans votre ACL Web. Pour une liste complète des options, reportez-vous aux sections Notions de base sur les énoncés etAction de la règle.

Pour définir vos critères d'inspection et de traitement des requêtes Web, effectuez les tâches suivantes :

1. Choisissez l'action par défaut de l'ACL WebBlock, Allow ou, pour les requêtes Web qui ne correspondent à aucune des règles que vous spécifiez. Pour plus d’informations, consultez L'action par défaut de l'ACL Web.
2. Ajoutez les groupes de règles que vous souhaitez utiliser dans votre liste ACL web. Les groupes de règles gérés contiennent généralement des règles qui bloquent les demandes web. Pour de plus amples informations sur les groupes de règles, reportez-vous à la section AWS WAF groupes de règles.
3. Spécifiez des critères de correspondance et des instructions de manipulation supplémentaires dans une ou plusieurs règles. Pour ajouter plusieurs règles, commencez par les instructions de `OR` règles `AND` ou imbriquez les règles que vous souhaitez combiner sous celles-ci. Si vous souhaitez annuler une option de règle, imbriquez la règle dans une instruction NOT. Le cas échéant, vous pouvez utiliser une règle basée sur la fréquence au lieu d'une règle régulière pour limiter le nombre de demandes provenant des adresses IP qui répondent aux conditions. Pour de plus amples informations sur les règles, veuillez consulter AWS WAF règles.

Si vous ajoutez plusieurs règles à une ACL Web, AWS WAF évalue les règles dans l'ordre dans lequel elles sont répertoriées pour l'ACL Web. Pour plus d’informations, consultez Évaluation des règles ACL Web et des groupes de règles.

Lorsque vous créez une liste ACL web, vous spécifiez les types de ressources avec lesquels vous souhaitez l'utiliser. Pour plus d’informations, veuillez consulter Création d'une liste ACL web. Après avoir défini une liste ACL web, vous pouvez l'associer à vos ressources pour commencer à leur fournir une protection. Pour plus d’informations, consultez Associer ou dissocier une ACL Web à une ressource AWS.

Comment AWS les ressources gèrent les délais de réponse dus à AWS WAF

Dans certains cas, une erreur interne AWS WAF peut retarder la réponse aux AWS ressources associées quant à l'autorisation ou au blocage d'une demande. Dans ces cas, il autorise CloudFront généralement la demande ou diffuse le contenu, tandis que les services régionaux refusent généralement la demande et ne diffusent pas le contenu.

Rubriques

Évaluation des règles ACL Web et des groupes de règles

La façon dont une liste ACL web gère une demande web dépend des éléments suivants :

- Les paramètres de priorité numérique des règles dans l'ACL Web et à l'intérieur des groupes de règles
- Les paramètres d'action sur les règles et la liste ACL web
- Toutes les dérogations que vous apportez aux règles des groupes de règles que vous ajoutez

Pour obtenir la liste des paramètres d'action des règles, consultezAction de la règle.

Vous pouvez personnaliser le traitement des demandes et des réponses dans les paramètres d'action de vos règles et dans les paramètres d'action ACL Web par défaut. Pour plus d’informations, consultez Demandes et réponses Web personnalisées dans AWS WAF.

Rubriques

Ordre de traitement des règles et des groupes de règles dans une ACL Web

Dans une ACL Web et au sein de n'importe quel groupe de règles, vous déterminez l'ordre d'évaluation des règles à l'aide de paramètres de priorité numériques. Vous devez attribuer à chaque règle d'une ACL Web un paramètre de priorité unique au sein de cette ACL Web, et vous devez attribuer à chaque règle d'un groupe de règles un paramètre de priorité unique au sein de ce groupe de règles.

> **Note**
>
> Lorsque vous gérez des groupes de règles et des ACL Web via la console, vous AWS WAF attribuez des paramètres de priorité numériques uniques en fonction de l'ordre des règles dans la liste. AWS WAF assigne la priorité numérique la plus faible à la règle en haut de la liste et la priorité numérique la plus élevée à la règle en bas.

Lorsqu'il AWS WAF évalue une ACL Web ou un groupe de règles par rapport à une requête Web, il évalue les règles à partir du paramètre de priorité numérique le plus bas jusqu'à ce qu'il trouve une correspondance qui met fin à l'évaluation ou épuise toutes les règles.

Supposons, par exemple, que votre ACL Web comporte les règles et groupes de règles suivants, classés par ordre de priorité comme indiqué ci-dessous :

- Règle 1 — priorité 0
- RuleGroupA — priorité 100
  - Règle A1 — priorité 10 000
  - Règle A2 — priorité 20 000
- Règle 2 — priorité 200
- RuleGroupB — priorité 300
  - Règle B1 — priorité 0
  - Règle B2 — priorité 1

AWS WAF évaluerait les règles de cette ACL Web dans l'ordre suivant :

- Règle 1
- RuleGroupA. Règle A1

- RuleGroupA. Règle A2
- Règle 2
- RuleGroupPar RuleB1
- RuleGroupPar RuleB2

Comment AWS WAF gère les règles et les actions de groupes de règles dans une ACL Web

Lorsque vous configurez vos règles et vos groupes de règles, vous choisissez la manière dont vous AWS WAF souhaitez gérer les requêtes Web correspondantes :

- Allowet Block mettent fin à des actions, Allow et les Block actions arrêtent tout autre traitement de l'ACL Web sur la requête Web correspondante. Si une règle d'une ACL Web trouve une correspondance pour une demande et que l'action de la règle est Allow ouBlock, cette correspondance détermine la disposition finale de la demande Web pour l'ACL Web. AWS WAF ne traite aucune autre règle de l'ACL Web qui vient après celle correspondante. Ceci est vrai pour les règles que vous ajoutez directement à la liste ACL web et pour les règles qui se trouvent dans un groupe de règles ajoutées. Avec cette Block action, la ressource protégée ne reçoit ni ne traite la demande Web.
- Countest une action sans fin : lorsqu'une règle comportant une Count action correspond à une demande, AWS WAF compte la demande, puis poursuit le traitement des règles qui suivent dans l'ensemble de règles ACL Web.
- CAPTCHAet il Challenge peut s'agir d'actions non résiliantes ou résilientes : lorsqu'une règle comportant l'une de ces actions correspond à une demande, AWS WAF vérifie le statut de son jeton. Si la demande contient un jeton valide, AWS WAF traite la correspondance comme une Count correspondance, puis poursuit le traitement des règles qui suivent dans l'ensemble de règles ACL Web. Si la demande ne contient pas de jeton valide, AWS WAF met fin à l'évaluation et envoie au client un casse-tête CAPTCHA ou un défi de session client en arrière-plan silencieux à résoudre.

Si l'évaluation des règles n'entraîne aucune action de fin, AWS WAF applique l'action par défaut de l'ACL Web à la demande. Pour plus d’informations, veuillez consulter L'action par défaut de l'ACL Web.

Dans votre ACL Web, vous pouvez remplacer les paramètres d'action des règles au sein d'un groupe de règles et vous pouvez annuler l'action renvoyée par un groupe de règles. Pour plus d'informations, veuillez consulter Options de dérogation aux actions pour les groupes de règles.

Interaction entre les actions et les paramètres de priorité

Les actions qui AWS WAF s'appliquent à une requête Web sont affectées par les paramètres de priorité numérique des règles de l'ACL Web. Par exemple, supposons que votre ACL Web possède une règle avec Allow action et une priorité numérique de 50 et une autre règle avec Count action et une priorité numérique de 100. AWS WAF évalue les règles d'une ACL Web dans l'ordre de leur priorité, en commençant par le paramètre le plus bas, afin d'évaluer la règle d'autorisation avant la règle de décompte. Une requête Web qui correspond aux deux règles correspondra d'abord à la règle d'autorisation. Comme Allow il s'agit d'une action terminale, elle AWS WAF arrêtera l'évaluation à cette correspondance et n'évaluera pas la demande par rapport à la règle du décompte.

- Si vous souhaitez uniquement inclure les demandes qui ne correspondent pas à la règle d'autorisation dans les statistiques de vos règles de comptage, les paramètres de priorité des règles fonctionneront.
- D'autre part, si vous souhaitez que les mesures de comptage soient issues de la règle de comptage, même pour les demandes correspondant à la règle d'autorisation, vous devez attribuer à la règle de comptage un paramètre de priorité numérique inférieur à celui de la règle d'autorisation, afin qu'elle s'exécute en premier.

Pour plus d'informations sur les paramètres de priorité, consultezOrdre de traitement des règles et des groupes de règles dans une ACL Web.

Options de dérogation aux actions pour les groupes de règles

Lorsque vous ajoutez un groupe de règles à votre ACL Web, vous pouvez annuler les actions qu'il effectue sur les requêtes Web correspondantes. Le fait de remplacer les actions d'un groupe de règles dans votre configuration ACL Web ne modifie pas le groupe de règles lui-même. Cela modifie uniquement la manière dont le groupe de règles est AWS WAF utilisé dans le contexte de l'ACL Web.

Les actions des règles du groupe de règles remplacent les actions

Vous pouvez remplacer les actions des règles au sein d'un groupe de règles par n'importe quelle action de règle valide. Dans ce cas, les demandes correspondantes sont traitées exactement comme si l'action de la règle configurée était le paramètre de remplacement.

> **Note**
>
> Les actions relatives aux règles peuvent être terminales ou non. Une action de terminaison arrête l'évaluation ACL Web de la demande et la laisse continuer vers votre application protégée ou la bloque.

Voici les options d'action de la règle :

- Allow— AWS WAF permet à la demande d'être transmise à la AWS ressource protégée pour traitement et réponse. Il s'agit d'une action terminale. Dans les règles que vous définissez, vous pouvez insérer des en-têtes personnalisés dans la demande avant de la transmettre à la ressource protégée.
- Block— AWS WAF bloque la demande. Il s'agit d'une action terminale. Par défaut, votre AWS ressource protégée répond par un code d'`403 (Forbidden)`état HTTP. Dans les règles que vous définissez, vous pouvez personnaliser la réponse. En cas de AWS WAF blocage d'une demande, les paramètres Block d'action déterminent la réponse que la ressource protégée renvoie au client.
- Count— AWS WAF compte la demande mais ne détermine pas s'il faut l'autoriser ou la bloquer. Il s'agit d'une action sans fin. AWS WAF continue de traiter les règles restantes dans l'ACL Web. Dans les règles que vous définissez, vous pouvez insérer des en-têtes personnalisés dans la demande et ajouter des libellés auxquels d'autres règles peuvent correspondre.
- CAPTCHAet Challenge — AWS WAF utilise des puzzles CAPTCHA et des défis silencieux pour vérifier que la demande ne provient pas d'un bot, et AWS WAF utilise des jetons pour suivre les récentes réponses positives des clients.

  Les puzzles CAPTCHA et les défis silencieux ne peuvent être exécutés que lorsque les navigateurs accèdent à des points de terminaison HTTPS. Les clients du navigateur doivent fonctionner dans des contextes sécurisés pour acquérir des jetons.

  > **Note**
  >
  > Des frais supplémentaires vous sont facturés lorsque vous utilisez l'action CAPTCHA ou la Challenge règle dans l'une de vos règles ou en tant que dérogation d'action de règle dans un groupe de règles. Pour plus d’informations, consultez Tarification d’AWS WAF.

  Ces actions de règles peuvent être terminales ou non, selon l'état du jeton dans la demande :

- Non résiliable pour un jeton valide et non expiré : si le jeton est valide et non expiré conformément au CAPTCHA configuré ou à la durée d'immunité au défi, AWS WAF gère la demande de la même manière que l'action. Count AWS WAF continue d'inspecter la requête Web en fonction des règles restantes de l'ACL Web. Comme pour la Count configuration, dans les règles que vous définissez, vous pouvez éventuellement configurer ces actions avec des en-têtes personnalisés à insérer dans la demande, et vous pouvez ajouter des étiquettes auxquelles d'autres règles peuvent correspondre.
- Terminer par une demande bloquée pour un jeton non valide ou expiré — Si le jeton n'est pas valide ou si l'horodatage indiqué est expiré, AWS WAF met fin à l'inspection de la requête Web et bloque la demande, comme dans le cas de l'action. Block AWS WAF répond ensuite au client avec un code de réponse personnalisé. En CAPTCHA effet, si le contenu de la demande indique que le navigateur client peut la gérer, AWS WAF envoie un casse-tête CAPTCHA dans un JavaScript interstitiel, conçu pour distinguer les clients humains des robots. Pour l'Challengeaction, AWS WAF envoie un JavaScript interstitiel avec un défi silencieux conçu pour distinguer les navigateurs normaux des sessions exécutées par des robots.

Pour plus d’informations, consultez CAPTCHAet Challenge dans AWS WAF.

Pour plus d'informations sur l'utilisation de cette option, consultezRemplacer les actions des règles dans un groupe de règles.

Remplacer l'action de la règle par Count

Le cas d'utilisation le plus courant des dérogations aux actions des règles est le remplacement de certaines ou de toutes les actions des règles afin Count de tester et de surveiller le comportement d'un groupe de règles avant de le mettre en production.

Vous pouvez également l'utiliser pour résoudre les problèmes liés à un groupe de règles qui génère des faux positifs. Les faux positifs se produisent lorsqu'un groupe de règles bloque le trafic que vous ne vous attendez pas à ce qu'il bloque. Si vous identifiez une règle au sein d'un groupe de règles susceptible de bloquer les demandes que vous souhaitez autoriser, vous pouvez maintenir le nombre d'actions annulées sur cette règle, afin de l'empêcher de donner suite à vos demandes.

Pour plus d'informations sur l'utilisation du remplacement des actions des règles lors des tests, consultezTester et ajuster vos AWS WAF protections.

Liste JSON : **`RuleActionOverrides`** remplace **`ExcludedRules`**

Si vous avez défini les actions de règles du groupe de règles sur Count dans votre configuration ACL Web avant le 27 octobre 2022, vous AWS WAF avez enregistré vos remplacements dans le JSON de l'ACL Web sous `ExcludedRules` le nom de. Désormais, le paramètre JSON permettant de remplacer une règle se Count trouve dans les `RuleActionOverrides` paramètres.

Lorsque vous utilisez la AWS WAF console pour modifier les paramètres du groupe de règles existant, la console convertit automatiquement tous `ExcludedRules` les paramètres du JSON en `RuleActionOverrides` paramètres, l'action de remplacement étant définie sur. Count

- Exemple de réglage actuel :

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

- Ancien exemple de réglage :

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

Nous vous recommandons de mettre à jour tous les `ExcludedRules` paramètres de vos listes JSON vers des `RuleActionOverrides` paramètres dont l'action est définie surCount. L'API accepte l'un ou l'autre paramètre, mais vous obtiendrez une cohérence dans vos listes JSON,

entre votre travail sur console et votre travail sur API, si vous utilisez uniquement le nouveau `RuleActionOverrides` paramètre.

L'action de retour du groupe de règles est remplacée par Count

Vous pouvez annuler l'action renvoyée par le groupe de règles en lui attribuant la valeur. Count

> **Note**
>
> Ce n'est pas une bonne option pour tester les règles d'un groupe de règles, car elle ne modifie pas la façon dont le groupe AWS WAF de règles est évalué lui-même. Cela n'affecte que le mode AWS WAF de gestion des résultats renvoyés à l'ACL Web à partir de l'évaluation du groupe de règles. Si vous souhaitez tester les règles dans un groupe de règles, utilisez l'option décrite dans la section précédente,Les actions des règles du groupe de règles remplacent les actions.

Lorsque vous remplacez l'action du groupe de règles parCount, AWS WAF traite l'évaluation du groupe de règles normalement.

Si aucune règle du groupe de règles ne correspond ou si toutes les règles correspondantes comportent une Count action, cette dérogation n'a aucun effet sur le traitement du groupe de règles ou de l'ACL Web.

La première règle du groupe de règles qui correspond à une requête Web et qui comporte une action de fin de règle entraîne AWS WAF l'arrêt de l'évaluation du groupe de règles et renvoie le résultat de l'action de fin au niveau d'évaluation de l'ACL Web. À ce stade, dans l'évaluation de l'ACL Web, cette dérogation prend effet. AWS WAF remplace l'action finale afin que le résultat de l'évaluation du groupe de règles ne soit qu'une Count action. AWS WAF poursuit ensuite le traitement du reste des règles dans l'ACL Web.

Pour plus d'informations sur l'utilisation de cette option, consultezRemplacer le résultat de l'évaluation d'un groupe de règles par Count.

L'action par défaut de l'ACL Web

Lorsque vous créez et configurez une ACL Web, vous devez définir l'action par défaut de l'ACL Web. AWS WAF applique cette action à toute requête Web qui passe par toutes les évaluations des règles de l'ACL Web sans qu'une action de fin ne lui soit appliquée. Une action de terminaison

arrête l'évaluation ACL Web de la demande et la laisse continuer vers votre application protégée ou la bloque. Pour plus d'informations sur les actions relatives aux règles, consultezAction de la règle.

L'action par défaut de l'ACL Web doit déterminer la disposition finale de la requête Web. Il s'agit donc d'une action terminale :

- Allow— Si vous souhaitez autoriser la plupart des utilisateurs à accéder à votre site Web, mais que vous souhaitez bloquer l'accès aux attaquants dont les demandes proviennent d'adresses IP spécifiées, ou dont les demandes semblent contenir du code SQL malveillant ou des valeurs spécifiques, choisissez Allow l'action par défaut. Ensuite, lorsque vous ajoutez des règles à votre liste ACL web, ajoutez des règles qui identifient et bloquent les demandes spécifiques que vous souhaitez bloquer. Avec cette action, vous pouvez insérer des en-têtes personnalisés dans la demande avant de la transmettre à la ressource protégée.
- Block— Si vous souhaitez empêcher la plupart des utilisateurs d'accéder à votre site Web, mais que vous souhaitez autoriser l'accès aux utilisateurs dont les demandes proviennent d'adresses IP spécifiées ou dont les demandes contiennent des valeurs spécifiées, choisissez Block l'action par défaut. Ensuite, lorsque vous ajoutez des règles à votre liste ACL web, ajoutez des règles qui identifient et autorisent les demandes spécifiques que vous souhaitez autoriser. Par défaut, pour l'Blockaction, la AWS ressource répond par un code d'`403 (Forbidden)`état HTTP, mais vous pouvez personnaliser la réponse.

Pour plus d'informations sur la personnalisation des demandes et des réponses, consultezDemandes et réponses Web personnalisées dans AWS WAF.

La configuration de vos propres règles et groupes de règles dépend en partie de l'autorisation ou du blocage de la plupart des demandes web. Par exemple, si vous souhaitez autoriser la plupart des demandes, vous devez définir l'action par défaut de l'ACL Web surAllow, puis ajouter des règles identifiant les demandes Web que vous souhaitez bloquer, telles que les suivantes :

- Les requêtes provenant d'adresses IP qui effectuent un trop grand nombre de requêtes
- Demandes en provenance de pays dans lesquels vous n'avez pas d'activité ou qui sont la source d'attaques fréquentes
- Les requêtes qui incluent des valeurs fausses dans l'en-tête `User-agent`
- Les requêtes qui semblent inclure du code SQL malveillant

Les règles des groupes de règles gérés utilisent généralement l'Blockaction, mais ce n'est pas le cas de toutes. Par exemple, certaines règles utilisées pour le contrôle des robots utilisent les paramètres

Challenge d'action CAPTCHA et. Pour de plus amples informations sur les groupes de règles gérées, reportez-vous à la section Groupes de règles gérés.

Gestion des limites de taille des organismes inspectés

La limite de taille d'inspection de la carrosserie est la taille maximale demandée AWS WAF pouvant être inspectée. Lorsque le corps d'une requête Web est supérieur à la limite, le service hôte sous-jacent ne transmet que le contenu se situant dans la limite à des AWS WAF fins d'inspection.

- Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko (8 192 octets).
- Pour API Gateway CloudFront, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko (16 384 octets), et vous pouvez augmenter la limite pour tous les types de ressources par incréments de 16 Ko, jusqu'à 64 Ko. Les options de configuration sont 16 Ko, 32 Ko, 48 Ko et 64 Ko.

Manipulation de carrosseries surdimensionnées

Si votre trafic Web inclut des corps dont la taille est supérieure à la limite, la gestion des surdimensionnements que vous avez configurée s'appliquera. Pour plus d'informations sur les options de gestion des surdimensionnements, consultezGestion des composants de demande surdimensionnés dans AWS WAF.

Considérations relatives à la tarification pour augmenter le montant des limites

AWS WAF facture un tarif de base pour l'inspection du trafic qui se situe dans la limite par défaut pour le type de ressource.

Pour les CloudFront ressources API Gateway, Amazon Cognito, App Runner et Verified Access, si vous augmentez le paramètre de limite, le trafic AWS WAF pouvant être inspecté inclut la taille corporelle jusqu'à votre nouvelle limite. Des frais supplémentaires vous sont facturés uniquement pour l'inspection des demandes dont la taille du corps est supérieure aux 16 Ko par défaut. Pour plus d'informations sur la tarification, consultez Tarification d'AWS WAF.

Options pour modifier la limite de taille d'inspection de la carrosserie

Vous pouvez configurer la limite de taille d'inspection corporelle pour les CloudFront ressources API Gateway, Amazon Cognito, App Runner ou Verified Access.

Lorsque vous créez ou modifiez une ACL Web, vous pouvez modifier les limites de taille d'inspection du corps dans la configuration de l'association de ressources. Pour l'API, consultez la configuration

d'association de l'ACL Web à l'adresse AssociationConfig. Pour la console, consultez la configuration sur la page où vous spécifiez les ressources associées à l'ACL Web. Pour obtenir des conseils sur la configuration de la console, consultezUtilisation des listes ACL web.

Configurations pour le CAPTCHA, le défi et les jetons

Vous pouvez configurer des options dans votre ACL Web pour les règles qui utilisent les actions de Challenge règles CAPTCHA ou pour les SDK d'intégration d'applications qui gèrent les défis clients silencieux pour les protections AWS WAF gérées.

Ces fonctionnalités atténuent l'activité des robots en lançant des puzzles CAPTCHA aux utilisateurs finaux et en proposant des défis silencieux aux sessions des clients. Lorsque le client répond avec succès, il AWS WAF fournit un jeton à utiliser dans sa demande Web, horodaté avec les dernières réponses au puzzle et au défi réussis. Pour plus d'informations, consultez AWS WAF Atténuation intelligente des menaces.

Dans votre configuration ACL Web, vous pouvez configurer le mode de AWS WAF gestion de ces jetons :

- Durée du CAPTCHA et de l'immunité aux défis : ces durées indiquent la durée de validité d'un CAPTCHA ou d'un horodatage de défi. Les paramètres ACL Web sont hérités par toutes les règles qui n'ont pas leurs propres paramètres de temps d'immunité configurés, ainsi que par les SDK d'intégration des applications. Pour plus d'informations, consultez Expiration de l'horodatage : durée d'immunité des AWS WAF jetons.
- Domaines de jetons : par défaut, AWS WAF accepte les jetons uniquement pour le domaine de la ressource à laquelle l'ACL Web est associée. Si vous configurez une liste de domaines de jetons, AWS WAF accepte les jetons pour tous les domaines de la liste et pour le domaine de la ressource associée. Pour plus d'informations, voir AWS WAF configuration de la liste de domaines du jeton ACL Web.

Utilisation des listes ACL web

Cette section décrit les procédures de création, de gestion et d'utilisation des ACL Web via la AWS console.

Pour chaque ACL Web que vous utilisez, vous pouvez accéder aux résumés des mesures de trafic Web sur la page de l'ACL Web dans la AWS WAF console, sous l'onglet Aperçu du trafic. Les tableaux de bord de la console fournissent des résumés en temps quasi réel des CloudWatch

métriques AWS WAF collectées par Amazon lors de l'évaluation du trafic Web de votre application. Pour plus d'informations sur les tableaux de bord, consultezTableaux de bord de présentation du trafic Web ACL. Pour plus d'informations sur la surveillance du trafic de votre ACL Web, consultezSurveillance et réglage.

> ⚠ Risque lié au trafic de production
>
> Avant de déployer des modifications dans votre ACL Web pour le trafic de production, testez-les et ajustez-les dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite vos règles mises à jour en mode décompte avec votre trafic de production avant de les activer. Pour de plus amples informations, consultez Tester et ajuster vos AWS WAF protections.

> ⓘ Note
>
> L'utilisation de plus de 1 500 WCU dans une ACL Web entraîne des coûts supérieurs au prix de base de l'ACL Web. Pour plus d'informations, veuillez consulter les sections AWS WAF unités de capacité ACL Web (WCU) et Tarification d'AWS WAF.

Incohérences temporaires lors des mises à jour

Lorsque vous créez ou modifiez une ACL Web ou d'autres AWS WAF ressources, les modifications mettent peu de temps à se propager à toutes les zones où les ressources sont stockées. Le temps de propagation peut aller de quelques secondes à plusieurs minutes.

Voici des exemples d'incohérences temporaires que vous pourriez remarquer lors de la propagation des modifications :

- Après avoir créé une ACL Web, si vous essayez de l'associer à une ressource, vous pouvez obtenir une exception indiquant que l'ACL Web n'est pas disponible.
- Une fois que vous avez ajouté un groupe de règles à une ACL Web, les nouvelles règles de groupe de règles peuvent être en vigueur dans une zone où l'ACL Web est utilisée et pas dans une autre.
- Une fois que vous avez modifié le paramètre d'une action de règle, vous pouvez voir l'ancienne action à certains endroits et la nouvelle action à d'autres.

- Après avoir ajouté une adresse IP à un ensemble d'adresses IP utilisé dans une règle de blocage, la nouvelle adresse peut être bloquée dans une zone alors qu'elle est toujours autorisée dans une autre.

Rubriques

Création d'une liste ACL web

Pour créer une nouvelle ACL Web, utilisez l'assistant de création d'une ACL Web en suivant la procédure décrite sur cette page.

> **Risque lié au trafic de production**
>
> Avant de déployer des modifications dans votre ACL Web pour le trafic de production, testez-les et ajustez-les dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite vos règles mises à jour en mode décompte en fonction de votre trafic de production avant de les activer. Pour de plus amples informations, consultez Tester et ajuster vos AWS WAF protections.

> **Note**
>
> L'utilisation de plus de 1 500 WCU dans une ACL Web entraîne des coûts supérieurs au prix de base de l'ACL Web. Pour plus d'informations, veuillez consulter les sections AWS WAF unités de capacité ACL Web (WCU) et Tarification d'AWS WAF.

Pour créer une liste ACL web

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

2. Choisissez Web ACLs (Listes ACL Web) dans le volet de navigation, puis Create web ACL (Créer une liste ACL Web).
3. Dans Nom (Nom), entrez le nom que vous souhaitez utiliser pour identifier cette liste ACL web.

   > **Note**
   >
   > Vous ne pouvez pas modifier le nom une fois que vous créez la liste ACL web.

4. (Facultatif) Pour Description - facultatif, entrez une description plus longue pour la liste ACL web si vous le souhaitez.
5. Pour le nom de la CloudWatch métrique, modifiez le nom par défaut le cas échéant. Suivez les instructions sur la console pour connaître les caractères valides. Le nom ne peut pas contenir de caractères spéciaux, d'espaces blancs ou de noms de métriques réservés AWS WAF, notamment « All » et « Default_Action ».

   > **Note**
   >
   > Vous ne pouvez pas modifier le nom de la CloudWatch métrique après avoir créé l'ACL Web.

6. Sous Type de ressource, choisissez la catégorie de AWS ressource que vous souhaitez associer à cette ACL Web, soit les CloudFront distributions Amazon, soit les ressources régionales. Pour plus d'informations, consultez Associer ou dissocier une ACL Web à une ressource AWS.
7. Pour Région, si vous avez choisi un type de ressource régional, choisissez la région dans laquelle vous AWS WAF souhaitez stocker l'ACL Web.

   Vous devez uniquement choisir cette option pour les types de ressources régionaux. Pour les CloudFront distributions, la région est codée en dur pour la région de l'est des États-Unis (Virginie du Nord)`us-east-1`, pour les applications Global (CloudFront).
8. (CloudFront, API Gateway, Amazon Cognito, App Runner et Verified Access) Pour la limite de taille d'inspection des demandes Web, facultatif, si vous souhaitez spécifier une autre limite de taille d'inspection corporelle, sélectionnez la limite. L'inspection d'une taille corporelle supérieure à 16 Ko par défaut peut entraîner des coûts supplémentaires. Pour de plus amples informations sur cette option, veuillez consulter Gestion des limites de taille des organismes inspectés.
9. (Facultatif) Pour les AWS ressources associées : facultatif. Si vous souhaitez spécifier vos ressources maintenant, choisissez Ajouter AWS des ressources. Dans la boîte de dialogue,

choisissez les ressources que vous souhaitez associer, puis cliquez sur Ajouter. AWS WAF vous renvoie à la page Describe Web ACL et aux AWS ressources associées.

10. Choisissez Suivant.
11. (Facultatif) Si vous souhaitez ajouter des groupes de règles gérées, dans la page Ajouter des règles et des groupes de règles, choisissez Ajouter des règles, puis Ajouter des groupes de règles gérées. Pour chaque groupe de règles gérées que vous souhaitez ajouter, procédez comme suit :

    a. Sur la page Ajouter des groupes de règles gérés, développez la liste des groupes de règles AWS gérés ou du AWS Marketplace vendeur de votre choix.

    b. Pour le groupe de règles que vous souhaitez ajouter, dans la colonne Action, activez le bouton Ajouter à l'ACL Web.

    Pour personnaliser la façon dont votre ACL Web utilise le groupe de règles, choisissez Modifier. Les paramètres de personnalisation courants sont les suivants :

    - Remplacez les actions des règles pour certaines ou toutes les règles. Si vous ne définissez pas d'action de remplacement pour une règle, l'évaluation utilise l'action de règle définie au sein du groupe de règles. Pour de plus amples informations sur cette option, veuillez consulter Options de dérogation aux actions pour les groupes de règles.
    - Réduisez la portée des requêtes Web inspectées par le groupe de règles en ajoutant une instruction scope-down. Pour de plus amples informations sur cette option, veuillez consulter Déclarations de portée réduite.
    - Certains groupes de règles gérés nécessitent que vous fournissiez une configuration supplémentaire. Consultez la documentation de votre fournisseur de groupes de règles gérés. Pour obtenir des informations spécifiques aux groupes de règles AWS gérées, consultezAWS Règles gérées pour AWS WAF.

    Lorsque vous avez terminé de définir vos paramètres, choisissez Enregistrer la règle.

    Choisissez Ajouter des règles pour terminer l'ajout de règles gérées et revenir à la page Ajouter des règles et des groupes de règles.

12. (Facultatif) Si vous souhaitez ajouter votre propre groupe de règles, sur la page Ajouter des règles et des groupes de règles, choisissez Ajouter des règles, puis Ajouter mes propres règles et groupes de règles. Pour chaque groupe de règles que vous souhaitez ajouter, procédez comme suit :

a. Sur la page Ajouter mes propres règles et groupes de règles choisissez Groupe de règles.

b. Dans Nom, entrez le nom que vous souhaitez utiliser pour la règle de groupe de règles dans cette ACL Web. N'utilisez pas de noms commençant par `AWSShield`,`PreFM`, ou`PostFM`. Ces chaînes sont réservées ou peuvent prêter à confusion avec les groupes de règles gérés pour vous par d'autres services. veuillez consulter Groupes de règles fournis par d'autres services.

c. Choisissez votre groupe de règles dans la liste.

> **Note**
>
> Si vous souhaitez annuler les actions des règles pour un groupe de règles qui vous est propre, enregistrez-le d'abord dans l'ACL Web, puis modifiez l'ACL Web et la déclaration de référence du groupe de règles dans la liste des règles de l'ACL Web. Vous pouvez remplacer les actions des règles par n'importe quel paramètre d'action valide, comme vous pouvez le faire pour les groupes de règles gérés.

d. Choisissez Ajouter une règle.

13. (Facultatif) Si vous souhaitez ajouter votre propre règle, sur la page Ajouter des règles et des groupes de règles, choisissez Ajouter des règles, Ajouter mes propres règles et groupes de règles, Générateur de règles, puis Éditeur visuel de règles.

> **Note**
>
> L'éditeur visuel de règles de la console prend en charge un niveau d'imbrication. Par exemple, vous pouvez utiliser une seule instruction logique `AND` ou une seule `OR` instruction et y imbriquer un niveau d'autres instructions, mais vous ne pouvez pas imbriquer des instructions logiques dans des instructions logiques. Pour gérer des instructions de règle plus complexes, utilisez l'éditeur JSON de règles. Pour de plus amples informations sur toutes les options des règles, reportez-vous à la section AWS WAF règles.
> Cette procédure couvre l'éditeur visuel de règles.

a. Dans la zone Nom, entrez le nom que vous souhaitez utiliser pour identifier cette règle. N'utilisez pas de noms commençant par `AWSShield`,`PreFM`, ou`PostFM`. Ces chaînes sont

réservées ou peuvent prêter à confusion avec les groupes de règles gérés pour vous par d'autres services.

b. Entrez la définition de votre règle, en fonction de vos besoins. Vous pouvez combiner des règles dans des instructions logiques AND et des instructions de OR règles. L'Assistant vous guide à travers les options de chaque règle, en fonction du contexte. Pour de plus amples informations sur les options de vos règles, reportez-vous à la section AWS WAF règles.

c. Dans Action, sélectionnez l'action que la règle doit effectuer lorsqu'elle correspond à une demande web. Pour de plus amples informations sur vos choix, veuillez consulter Action de la règle et Évaluation des règles ACL Web et des groupes de règles.

Si vous utilisez l'Challengeaction CAPTCHAou, ajustez la configuration du temps d'immunité en fonction des besoins de la règle. Si vous ne spécifiez pas le paramètre, la règle hérite de l'ACL Web. Pour modifier les paramètres de durée d'immunité de l'ACL Web, modifiez l'ACL Web après l'avoir créée. Pour plus d'informations sur les durées d'immunité, consultezExpiration de l'horodatage : durée d'immunité des AWS WAF jetons.

> **Note**
>
> Des frais supplémentaires vous sont facturés lorsque vous utilisez l'action CAPTCHA ou la Challenge règle dans l'une de vos règles ou en tant que dérogation d'action de règle dans un groupe de règles. Pour plus d’informations, consultez Tarification d’AWS WAF.

Si vous souhaitez personnaliser la demande ou la réponse, choisissez les options correspondantes et renseignez les détails de votre personnalisation. Pour plus d’informations, consultez Demandes et réponses Web personnalisées dans AWS WAF.

Si vous souhaitez que votre règle ajoute des étiquettes aux requêtes Web correspondantes, choisissez les options correspondantes et renseignez les détails de votre étiquette. Pour plus d’informations, consultez AWS WAF étiquettes sur les requêtes Web.

d. Choisissez Ajouter une règle.

14. Choisissez l'action par défaut pour l'ACL Web, Block soitAllow. Il s'agit de l'action qui AWS WAF exécute une demande lorsque les règles de l'ACL Web ne l'autorisent ou ne la bloquent pas explicitement. Pour plus d’informations, consultez L'action par défaut de l'ACL Web.

Si vous souhaitez personnaliser l'action par défaut, choisissez les options correspondantes et renseignez les détails de votre personnalisation. Pour plus d'informations, consultez Demandes et réponses Web personnalisées dans AWS WAF.

15. Vous pouvez définir une liste de domaines de jetons pour permettre le partage de jetons entre les applications protégées. Les jetons sont utilisés par les Challenge actions CAPTCHA et par les SDK d'intégration d'applications que vous implémentez lorsque vous utilisez les groupes de règles AWS gérées pour la création de comptes AWS WAF Fraud Control, la prévention des fraudes (ACFP), la prévention des AWS WAF fraudes (ATP) et le contrôle des AWS WAF bots.

    Les suffixes publics ne sont pas autorisés. Par exemple, vous ne pouvez pas utiliser `gov.au` ou en `co.uk` tant que domaine de jetons.

    Par défaut, AWS WAF accepte les jetons uniquement pour le domaine de la ressource protégée. Si vous ajoutez des domaines de jetons dans cette liste, AWS WAF les jetons sont acceptés pour tous les domaines de la liste et pour le domaine de la ressource associée. Pour plus d'informations, consultez AWS WAF configuration de la liste de domaines du jeton ACL Web.

16. Choisissez Suivant.
17. Sur la page Définir la priorité des règles, sélectionnez et déplacez vos règles et groupes de règles dans l'ordre dans lequel vous AWS WAF souhaitez les traiter. AWS WAF traite les règles en commençant par le haut de la liste. Lorsque vous enregistrez, l'ACL Web AWS WAF attribue des paramètres de priorité numériques aux règles, dans l'ordre dans lequel vous les avez listés. Pour plus d'informations, consultez Ordre de traitement des règles et des groupes de règles dans une ACL Web.
18. Choisissez Suivant.
19. Sur la page Configurer les métriques, passez en revue les options et appliquez les mises à jour dont vous avez besoin. Vous pouvez combiner des métriques provenant de plusieurs sources en leur attribuant le même nom de CloudWatch métrique.
20. Choisissez Suivant.
21. Dans la page Réviser et créer une liste ACL web, vérifiez vos définitions. Si vous souhaitez modifier une zone, choisissez Modifier pour la zone. Vous êtes alors renvoyé à la page de l'Assistant ACL web. Effectuez les modifications, puis choisissez Suivant dans les pages jusqu'à ce que vous reveniez à la page Réviser et créer une liste ACL web.
22. Sélectionnez Create web ACL. Votre nouvelle liste ACL web est répertoriée dans la page Liste ACL web.

Modification d'une ACL Web

Pour ajouter ou supprimer des règles dans une ACL Web ou modifier les paramètres de configuration, accédez à l'ACL Web en suivant la procédure décrite sur cette page. Lors de la mise à jour d'une ACL Web, AWS WAF fournit une couverture continue aux ressources que vous avez associées à l'ACL Web.

> **Risque lié au trafic de production**
>
> Avant de déployer des modifications dans votre ACL Web pour le trafic de production, testez-les et ajustez-les dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite vos règles mises à jour en mode décompte en fonction de votre trafic de production avant de les activer. Pour de plus amples informations, consultez Tester et ajuster vos AWS WAF protections.

> **Note**
>
> L'utilisation de plus de 1 500 WCU dans une ACL Web entraîne des coûts supérieurs au prix de base de l'ACL Web. Pour plus d'informations, veuillez consulter les sections AWS WAF unités de capacité ACL Web (WCU) et Tarification d'AWS WAF.

Pour modifier une liste ACL web

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, choisissez Web ACLs.
3. Choisissez le nom de la liste ACL web que vous voulez modifier. La console vous amène à la description de l'ACL Web.

   > **Note**
   >
   > Les ACL Web gérées par AWS Firewall Manager ont des noms commençant par. `FMManagedWebACLV2-` L'administrateur de Firewall Manager les gère dans les AWS WAF politiques de Firewall Manager. Ces listes ACL web peuvent contenir des ensembles de groupes de règles qui sont désignés pour s'exécuter en premier et en dernier dans la liste ACL web, de part et d'autre des règles ou groupes de règles que

vous ajoutez et gérez. Vous ne pouvez modifier aucune de ces spécifications du premier et du dernier groupe de règles. Le premier et le dernier groupe de règles ont des noms commençant respectivement par `PREFMManaged-` et`POSTFMManaged-`. Pour plus d'informations sur ces stratégies, consultez AWS WAF politiques.

4. Modifiez l'ACL Web selon vos besoins. Sélectionnez les onglets correspondant aux zones de configuration qui vous intéressent et modifiez les paramètres modifiables. Pour chaque paramètre que vous modifiez, lorsque vous choisissez Enregistrer et que vous revenez à la page de description de l'ACL Web, la console enregistre vos modifications dans l'ACL Web.

   Vous trouverez ci-dessous la liste des onglets contenant les composants de configuration de l'ACL Web.

   - Onglet Règles
     - Règles définies dans l'ACL Web — Vous pouvez modifier et gérer les règles que vous avez définies dans l'ACL Web de la même manière que lors de la création de l'ACL Web.

       > **Note**
       >
       > Ne modifiez pas le nom des règles que vous n'avez pas ajoutées manuellement à votre ACL Web. Si vous utilisez d'autres services pour gérer les règles à votre place, le fait de changer leur nom pourrait supprimer ou diminuer leur capacité à fournir les protections prévues. AWS Shield Advanced et AWS Firewall Manager les deux créent des règles dans votre ACL Web. Pour plus d'informations, consultez Groupes de règles fournis par d'autres services.

       > **Note**
       >
       > Si vous modifiez le nom d'une règle et que vous souhaitez que le nom de la métrique de la règle reflète le changement, vous devez également mettre à jour le nom de la métrique. AWS WAF ne met pas automatiquement à jour le nom de la métrique d'une règle lorsque vous modifiez le nom de la règle. Vous pouvez modifier le nom de la métrique lorsque vous modifiez la règle dans la console, à l'aide de l'éditeur JSON de règles. Vous pouvez également modifier les deux noms via les API et dans toute liste JSON que vous utilisez pour définir votre ACL Web ou votre groupe de règles.

Pour plus d'informations sur les règles et les paramètres des groupes de règles, reportez-vous AWS WAF règles aux sections etAWS WAF groupes de règles.

- Unités de capacité de la règle ACL Web utilisées : utilisation actuelle de la capacité de votre ACL Web. Il s'agit d'une vue uniquement.
- Action ACL Web par défaut pour les demandes qui ne correspondent à aucune règle — Pour plus d'informations sur ce paramètre, consultezL'action par défaut de l'ACL Web.
- Configurations de CAPTCHA et de défi ACL Web : ces durées d'immunité déterminent la durée de validité d'un CAPTCHA ou d'un jeton de défi après son acquisition. Vous ne pouvez modifier ce paramètre ici qu'après avoir créé l'ACL Web. Pour plus d'informations sur ces paramètres, consultez Expiration de l'horodatage : durée d'immunité des AWS WAF jetons.
- Liste de domaines de jetons : AWS WAF accepte les jetons pour tous les domaines de la liste et pour le domaine de la ressource associée. Pour plus d'informations, consultez AWS WAF configuration de la liste de domaines du jeton ACL Web.

- AWS Onglet Ressources associées
  - Limite de taille d'inspection des requêtes Web : incluse uniquement pour les ACL Web qui protègent les CloudFront distributions. La limite de taille limite pour l'inspection de la carrosserie détermine la quantité de composant de carrosserie à AWS WAF envoyer pour inspection. Pour plus d'informations sur ce paramètre, consultez Gestion des limites de taille des organismes inspectés.
  - AWS Ressources associées : liste des ressources auxquelles l'ACL Web est actuellement associée et qu'elle protège. Vous pouvez localiser des ressources situées dans la même région que l'ACL Web et les associer à l'ACL Web. Pour plus d'informations, consultez Associer ou dissocier une ACL Web à une ressource AWS.
- Onglet corps de réponse personnalisés
  - Corps de réponse personnalisés pouvant être utilisés par vos règles ACL Web dont l'action est définie surBlock. Pour plus d'informations, consultez Réponses personnalisées pour les Block actions.
- Onglet Journalisation et statistiques
  - Journalisation : journalisation du trafic évalué par l'ACL Web. Pour plus d'informations, consultez Journalisation AWS WAF du trafic ACL Web.

- Exemples de demandes : informations sur les règles qui correspondent aux requêtes Web. Pour plus d'informations sur l'affichage des exemples de demandes, consultezAffichage d'un exemple de demandes web.
- CloudWatch métriques — Mesures relatives aux règles de votre ACL Web. Pour plus d'informations sur CloudWatch les métriques Amazon, consultezSurveillance avec Amazon CloudWatch.

Incohérences temporaires lors des mises à jour

Lorsque vous créez ou modifiez une ACL Web ou d'autres AWS WAF ressources, les modifications mettent peu de temps à se propager à toutes les zones où les ressources sont stockées. Le temps de propagation peut aller de quelques secondes à plusieurs minutes.

Voici des exemples d'incohérences temporaires que vous pourriez remarquer lors de la propagation des modifications :

- Après avoir créé une ACL Web, si vous essayez de l'associer à une ressource, vous pouvez obtenir une exception indiquant que l'ACL Web n'est pas disponible.
- Une fois que vous avez ajouté un groupe de règles à une ACL Web, les nouvelles règles de groupe de règles peuvent être en vigueur dans une zone où l'ACL Web est utilisée et pas dans une autre.
- Une fois que vous avez modifié le paramètre d'une action de règle, vous pouvez voir l'ancienne action à certains endroits et la nouvelle action à d'autres.
- Après avoir ajouté une adresse IP à un ensemble d'adresses IP utilisé dans une règle de blocage, la nouvelle adresse peut être bloquée dans une zone alors qu'elle est toujours autorisée dans une autre.

Gestion du comportement d'un groupe de règles dans une liste ACL web

Cette section décrit vos options pour modifier la façon dont vous utilisez un groupe de règles dans votre liste ACL web. Ces informations s'appliquent à tous les types de groupe de règles. Après avoir ajouté un groupe de règles à une ACL Web, vous pouvez remplacer les actions des règles individuelles du groupe de règles par tout autre paramètre Count d'action de règle valide. Vous pouvez également annuler l'action résultante du groupe de règlesCount, ce qui n'a aucun effet sur la manière dont les règles sont évaluées au sein du groupe de règles.

Pour de plus amples informations sur ces options, consultez Options de dérogation aux actions pour les groupes de règles.

Remplacer les actions des règles dans un groupe de règles

Pour chaque groupe de règles d'une ACL Web, vous pouvez remplacer les actions de la règle contenue pour certaines ou toutes les règles.

Le cas d'utilisation le plus courant consiste à remplacer les actions des règles pour Count tester des règles nouvelles ou mises à jour. Si les métriques sont activées, vous recevez des métriques pour chaque règle que vous remplacez. Pour plus d'informations sur les tests, consultez Tester et ajuster vos AWS WAF protections.

Pour annuler les actions des règles dans un groupe de règles

Vous pouvez apporter ces modifications lorsque vous ajoutez un groupe de règles géré à l'ACL Web, et vous pouvez les appliquer à n'importe quel type de groupe de règles lorsque vous modifiez l'ACL Web. Ces instructions concernent un groupe de règles qui a déjà été ajouté à l'ACL Web. Consultez des informations supplémentaires sur cette option à l'adresseLes actions des règles du groupe de règles remplacent les actions.

1. Modifiez l'ACL Web.
2. Dans l'onglet Règles de la page Web ACL, sélectionnez le groupe de règles, puis choisissez Modifier.
3. Dans la section Règles du groupe de règles, gérez les paramètres d'action selon vos besoins.

   - Toutes les règles : pour définir une action de dérogation pour toutes les règles du groupe de règles, ouvrez le menu déroulant Annuler toutes les actions de règles et sélectionnez l'action de dérogation. Pour supprimer les dérogations pour toutes les règles, sélectionnez Supprimer toutes les dérogations.
   - Règle unique : pour définir une action de dérogation pour une seule règle, ouvrez le menu déroulant de la règle et sélectionnez l'action de dérogation. Pour supprimer une dérogation pour une règle, ouvrez le menu déroulant de la règle et sélectionnez Supprimer la dérogation.
4. Lorsque vous avez terminé d'apporter vos modifications, choisissez Enregistrer la règle. Les paramètres d'action de règle et d'action de remplacement sont répertoriés sur la page du groupe de règles.

L'exemple de liste JSON suivant montre une déclaration de groupe de règles dans une ACL Web qui remplace les actions des règles par Count pour les règles `CategoryVerifiedSearchEngine` et`CategoryVerifiedSocialMedia`. Dans le JSON, vous pouvez annuler toutes les actions des règles en fournissant une `RuleActionOverrides` entrée pour chaque règle individuelle.

```
{
    "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"
   }
}
```

Remplacer le résultat de l'évaluation d'un groupe de règles par Count

Vous pouvez annuler l'action qui résulte de l'évaluation d'un groupe de règles, sans modifier la façon dont les règles du groupe de règles sont configurées ou évaluées. Cette option n'est pas couramment utilisée. Si l'une des règles du groupe de règles aboutit à une correspondance, cette dérogation définit l'action résultante du groupe de règles surCount.

> **Note**
>
> Il s'agit d'un cas d'utilisation peu courant. La plupart des remplacements d'actions sont effectués au niveau de la règle, au sein du groupe de règles, comme décrit dansRemplacer les actions des règles dans un groupe de règles.

Vous pouvez annuler l'action résultante du groupe de règles dans l'ACL Web lorsque vous ajoutez ou modifiez le groupe de règles. Dans la console, ouvrez le volet facultatif de l'action Remplacer le groupe de règles du groupe de règles et activez le remplacement. Dans le JSON défini `0verrideAction` dans l'instruction du groupe de règles, comme indiqué dans l'exemple de liste suivant :

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

Associer ou dissocier une ACL Web à une ressource AWS

Vous pouvez l'utiliser AWS WAF pour créer les associations suivantes entre les ACLS Web et vos ressources :

- Associez une ACL Web régionale à l'une des ressources régionales répertoriées ci-dessous. Pour cette option, l'ACL Web doit se trouver dans la même région que votre ressource.
  - API REST d'Amazon API Gateway

  - Application Load Balancer
  - AWS AppSync API GraphQL
  - Groupe d'utilisateurs Amazon Cognito
  - AWS App Runner service
  - AWS Instance d'accès vérifié
- Associez une ACL Web globale à une CloudFront distribution Amazon. L'ACL Web mondial comportera une région codée en dur de l'est des États-Unis (Virginie du Nord).

Vous pouvez également associer une ACL Web à une CloudFront distribution lorsque vous créez ou mettez à jour la distribution elle-même. Pour plus d'informations, consultez la section Utiliser AWS WAF pour contrôler l'accès à votre contenu dans le manuel Amazon CloudFront Developer Guide.

Restrictions sur les associations multiples

Vous pouvez associer une seule ACL Web à une ou plusieurs AWS ressources, conformément aux restrictions suivantes :

- Vous ne pouvez associer chaque AWS ressource qu'à une seule ACL Web. La relation entre l'ACL Web et AWS les ressources est one-to-many.
- Vous pouvez associer une ACL Web à une ou plusieurs CloudFront distributions. Vous ne pouvez associer une ACL Web que vous avez associée à une CloudFront distribution à aucun autre type de AWS ressource.

Restrictions supplémentaires

Les restrictions supplémentaires suivantes s'appliquent aux associations ACL Web :

- Vous ne pouvez associer une ACL Web qu'à un Application Load Balancer qu'il contient. Régions AWS Par exemple, vous ne pouvez pas associer une ACL Web à un Application Load Balancer activé. AWS Outposts
- Vous ne pouvez pas associer un groupe d'utilisateurs Amazon Cognito à une ACL Web qui utilise le groupe de règles géré AWS WAF Fraud Control pour la création de comptes et prévention de la fraude (ACFP) `AWSManagedRulesACFPRuleSet` ou le groupe de règles géré AWS WAF contre le rachat de comptes Fraud Control (ATP). `AWSManagedRulesATPRuleSet` Pour plus d'informations sur la prévention de la fraude lors de la création de comptes, consultezAWS WAF Contrôle des fraudes : création de comptes, prévention des fraudes (ACFP). Pour plus

d'informations sur la prévention du piratage de compte, consultezAWS WAF Contrôle des fraudes et prévention des prises de contrôle des comptes (ATP).

⚠ Risque lié au trafic de production

Avant de déployer votre ACL Web pour le trafic de production, testez-la et ajustez-la dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite vos règles en mode comptage avec votre trafic de production avant de les activer. Pour de plus amples informations, consultez Tester et ajuster vos AWS WAF protections.

Pour associer une ACL Web à une AWS ressource

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, choisissez Web ACLs.
3. Choisissez le nom de l'ACL Web que vous souhaitez associer à une ressource. La console vous amène à la description de la liste ACL web, où vous pouvez la modifier.
4. Dans l'onglet AWS Ressources associées, choisissez Ajouter AWS des ressources.
5. Lorsque vous y êtes invité, choisissez le type de ressource, sélectionnez le bouton radio à côté de la ressource que vous souhaitez associer, puis choisissez Ajouter.

Pour dissocier une ACL Web d'une ressource AWS

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, choisissez Web ACLs.
3. Choisissez le nom de l'ACL Web que vous souhaitez dissocier de votre ressource. La console vous amène à la description de la liste ACL web, où vous pouvez la modifier.
4. Dans l'onglet AWS Ressources associées, sélectionnez la ressource dont vous souhaitez dissocier cette ACL Web.

> **Note**
>
> Vous devez dissocier une ressource à la fois. Ne choisissez pas plusieurs ressources.

5. Choisissez Dissocier. La console ouvre une boîte de dialogue de confirmation. Confirmez votre choix de dissocier l'ACL Web de la AWS ressource.

Supprimer une ACL Web

Pour supprimer une ACL Web, vous devez d'abord dissocier toutes les AWS ressources de l'ACL Web. Utilisez la procédure suivante.

Supprimer une liste ACL web

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, choisissez Web ACLs.
3. Sélectionnez le nom de la liste ACL web que vous souhaitez supprimer. La console vous amène à la description de la liste ACL web, où vous pouvez la modifier.
4. Dans l'onglet AWS Ressources associées, pour chaque ressource associée, sélectionnez le bouton radio à côté du nom de la ressource, puis choisissez Dissocier. Cela dissocie l'ACL Web de vos AWS ressources.
5. Dans le volet de navigation, choisissez Web ACLs.
6. Sélectionnez la case d'option en regard de la liste ACL web que vous supprimez, puis choisissez Supprimer.

AWS WAF groupes de règles

Un groupe de règles est un ensemble de règles réutilisables que vous pouvez ajouter à une liste ACL Web. Pour en savoir plus sur les listes ACL, veuillez consulter AWS WAF listes de contrôle d'accès Web (ACL Web).

Les groupes de règles se répartissent dans les principales catégories suivantes :

- Vos propres groupes de règles, que vous créez et gérez.

- Groupes de règles AWS gérés que les équipes chargées des règles gérées créent et gèrent pour vous.
- Groupes de règles gérés que AWS Marketplace les vendeurs créent et gèrent pour vous.
- Groupes de règles détenus et gérés par d'autres services tels que AWS Firewall Manager Shield Advanced.

Différences entre les groupes de règles et les listes ACL web

Les groupes de règles et les listes ACL web contiennent tous deux des règles, qui sont définies de la même manière aux deux endroits. Les groupes de règles diffèrent des listes ACL web selon les points suivants :

- Les groupes de règles ne peuvent pas contenir d'instructions de référence de groupes de règles.
- Vous pouvez réutiliser un seul groupe de règles dans plusieurs listes ACL web en ajoutant une instruction de référence de groupe de règles à chaque liste ACL web. Vous ne pouvez pas réutiliser une liste ACL Web.
- Les groupes de règles n'ont pas d'actions par défaut. Dans une liste ACL Web, vous définissez une action par défaut pour chaque règle ou groupe de règles que vous incluez. Chaque règle individuelle à l'intérieur d'un groupe de règles ou d'une liste ACL web a une action définie.
- Vous n'associez pas directement un groupe de règles à une AWS ressource. Pour protéger les ressources à l'aide d'un groupe de règles, vous utilisez le groupe de règles dans une liste ACL web.
- Les ACL Web ont une capacité maximale définie par le système de 5 000 unités de capacité ACL Web (WCU). Chaque groupe de règles possède un paramètre WCU qui doit être défini lors de sa création. Vous pouvez utiliser ce paramètre pour calculer les besoins de capacité supplémentaires que l'utilisation d'un groupe de règles ajouterait à votre liste ACL web. Pour plus d'informations sur les WCU, consultezAWS WAF unités de capacité ACL Web (WCU).

Pour de plus amples informations sur les règles, veuillez consulter AWS WAF règles.

Cette section fournit des conseils pour créer et gérer vos propres groupes de règles, décrit les groupes de règles gérés mis à votre disposition et fournit des conseils sur l'utilisation des groupes de règles gérés.

Rubriques

- Groupes de règles gérés

- Gestion de vos propres groupes de règles
- Groupes de règles fournis par d'autres services

Groupes de règles gérés

Les groupes de règles gérés sont des ensembles de ready-to-use règles prédéfinies que AWS AWS Marketplace les vendeurs rédigent et mettent à jour pour vous. La AWS WAF tarification de base s'applique à votre utilisation de n'importe quel groupe de règles géré. Pour plus d'informations sur les AWS WAF tarifs, consultez la section AWS WAF Tarification.

- Les groupes de règles AWS gérées pour le contrôle des AWS WAF bots, la prévention du rachat de comptes AWS WAF Fraud Control (ATP) et la prévention des AWS WAF fraudes liées à la création de comptes Fraud Control (ACFP) sont disponibles moyennant des frais supplémentaires, au-delà des AWS WAF frais de base. Pour plus d'informations sur la tarification, consultez la page AWS WAF Pricing (Tarification).
- Tous les autres groupes de règles AWS gérées sont disponibles pour AWS WAF les clients sans frais supplémentaires.
- AWS Marketplace les groupes de règles gérés sont disponibles par abonnement via AWS Marketplace. Chacun de ces groupes de règles est détenu et géré par le AWS Marketplace vendeur. Pour obtenir des informations sur les prix relatifs à l'utilisation d'un groupe de règles AWS Marketplace géré, contactez le AWS Marketplace vendeur.

Certains groupes de règles gérés sont conçus pour protéger des types spécifiques d'applications Web telles que WordPress Joomla ou PHP. D'autres offrent une protection étendue contre les menaces connues ou les vulnérabilités courantes des applications Web, notamment certaines de celles répertoriées dans le Top 10 de l'OWASP. Si vous êtes soumis à des conformités réglementaires telles que PCI et HIPAA, vous pouvez utiliser les groupes de règles gérées pour satisfaire les exigences de pare-feu des applications web.

Mises à jour automatiques

La mise à jour dans le contexte d'un paysage de menaces en constante évolution peut prendre du temps et coûter cher. Les groupes de règles gérés peuvent vous faire gagner du temps lors de leur mise en œuvre et de leur utilisation AWS WAF. De nombreux AWS AWS Marketplace vendeurs mettent automatiquement à jour les groupes de règles gérés et fournissent de nouvelles versions des groupes de règles lorsque de nouvelles vulnérabilités et menaces apparaissent.

Dans certains cas, AWS est informée des nouvelles vulnérabilités avant leur divulgation publique, en raison de sa participation à un certain nombre de communautés de divulgation privées. Dans ces cas, AWS vous pouvez mettre à jour les groupes de règles AWS gérées et les déployer pour vous avant même qu'une nouvelle menace ne soit connue.

Accès restreint aux règles d'un groupe de règles géré

Chaque groupe de règles géré fournit une description complète des types d'attaques et de vulnérabilités contre lesquels il est conçu pour se protéger. Pour protéger la propriété intellectuelle des fournisseurs de groupes de règles, vous ne pouvez pas consulter tous les détails des règles individuelles au sein d'un groupe de règles. Cette restriction permet également d'empêcher les utilisateurs malveillants de concevoir des menaces qui contournent les règles publiées.

Rubriques

- Groupes de règles gérés versionnés
- Utilisation des groupes de règles gérés
- AWS Règles gérées pour AWS WAF
- AWS Marketplace groupes de règles gérés

Groupes de règles gérés versionnés

De nombreux fournisseurs de groupes de règles gérés utilisent le versionnement pour mettre à jour les options et les fonctionnalités d'un groupe de règles. En général, une version spécifique d'un groupe de règles géré est statique. Parfois, un fournisseur peut avoir besoin de mettre à jour certaines ou toutes les versions statiques d'un groupe de règles géré, par exemple pour répondre à une menace de sécurité émergente.

Lorsque vous utilisez un groupe de règles gérées versionnées dans votre ACL Web, vous pouvez sélectionner la version par défaut et laisser le fournisseur gérer la version statique que vous utilisez, ou vous pouvez sélectionner une version statique spécifique.

Vous ne trouvez pas la version que vous recherchez ?

Si aucune version ne figure dans la liste des versions d'un groupe de règles, il est probable qu'elle arrive à expiration ou qu'elle a déjà expiré. Une fois l'expiration d'une version programmée, vous AWS WAF ne pouvez plus la choisir pour le groupe de règles.

Notifications SNS pour les AWS groupes de règles gérées

Les groupes de règles AWS gérées fournissent tous des notifications de version et de mise à jour SNS, à l'exception du groupe de règles de réputation IP. Les groupes de règles AWS gérées qui fournissent des notifications utilisent tous la même rubrique SNS : Amazon Resource Name (ARN). Pour vous inscrire aux notifications SNS, consultezÊtre informé des nouvelles versions et mises à jour.

Rubriques

- Cycle de vie des versions pour les groupes de règles gérés
- Expiration de version pour les groupes de règles gérés
- Meilleures pratiques pour gérer les versions de groupes de règles gérés

Cycle de vie des versions pour les groupes de règles gérés

Les fournisseurs gèrent les étapes du cycle de vie suivantes d'une version statique d'un groupe de règles géré :

- Publication et mises à jour : un fournisseur de groupes de règles gérés annonce les versions statiques à venir et les nouvelles versions statiques de ses groupes de règles gérés par le biais de notifications adressées à une rubrique Amazon Simple Notification Service (Amazon SNS). Les fournisseurs peuvent également utiliser cette rubrique pour communiquer d'autres informations importantes concernant leurs groupes de règles, telles que les mises à jour urgentes requises.

  Vous pouvez vous abonner à la rubrique du groupe de règles et configurer la manière dont vous souhaitez recevoir les notifications. Pour plus d’informations, consultez Être informé des nouvelles versions et mises à jour.
- Planification de l'expiration : un fournisseur de groupes de règles gérés planifie l'expiration des anciennes versions d'un groupe de règles. Une version dont l'expiration est prévue ne peut pas être ajoutée à vos règles ACL Web. Une fois l'expiration programmée pour une version, AWS WAF suit l'expiration à l'aide d'un compte à rebours sur Amazon CloudWatch.
- Expiration de version : si une ACL Web est configurée pour utiliser une version expirée d'un groupe de règles géré, elle AWS WAF utilise la version par défaut du groupe de règles lors de l'évaluation de l'ACL Web. AWS WAF Bloque également toutes les mises à jour de l'ACL Web qui ne suppriment pas le groupe de règles ou ne modifient pas sa version pour une version non expirée.

Si vous utilisez des groupes de règles AWS Marketplace gérés, demandez au fournisseur des informations supplémentaires sur le cycle de vie des versions.

Expiration de version pour les groupes de règles gérés

Si vous utilisez une version spécifique d'un groupe de règles, assurez-vous de ne pas continuer à utiliser une version au-delà de sa date d'expiration. Vous pouvez surveiller l'expiration des versions via les notifications SNS du groupe de règles et via les CloudWatch métriques Amazon.

Si une version que vous utilisez dans une ACL Web est expirée, AWS WAF bloque toutes les mises à jour de l'ACL Web qui n'incluent pas le déplacement du groupe de règles vers une version non expirée. Vous pouvez mettre à jour le groupe de règles vers une version disponible ou le supprimer de votre ACL Web.

La gestion de l'expiration pour un groupe de règles géré dépend du fournisseur du groupe de règles. Pour les groupes de règles AWS gérées, une version expirée est automatiquement remplacée par la version par défaut du groupe de règles. Pour les groupes de AWS Marketplace règles, demandez au fournisseur comment il gère l'expiration.

Lorsque le fournisseur crée une nouvelle version du groupe de règles, il définit la durée de vie prévue de la version. Bien que l'expiration de la version ne soit pas prévue, la valeur de la CloudWatch métrique Amazon est définie en fonction du paramètre de durée de vie CloudWatch prévisionnelle, et vous verrez une valeur fixe pour la métrique. Une fois que le fournisseur a programmé l'expiration de la métrique, la valeur de la métrique diminue chaque jour jusqu'à atteindre zéro le jour de l'expiration. Pour plus d'informations sur le suivi de l'expiration, consultezExpiration des versions de suivi.

Meilleures pratiques pour gérer les versions de groupes de règles gérés

Suivez ce guide de bonnes pratiques pour gérer le versionnement lorsque vous utilisez un groupe de règles géré versionné.

Lorsque vous utilisez un groupe de règles géré dans votre ACL Web, vous pouvez choisir d'utiliser une version statique spécifique du groupe de règles, ou vous pouvez choisir d'utiliser la version par défaut :

- Version par défaut : définit AWS WAF toujours la version par défaut sur la version statique actuellement recommandée par le fournisseur. Lorsque le fournisseur met à jour sa version statique recommandée, met AWS WAF automatiquement à jour le paramètre de version par défaut pour le groupe de règles dans votre ACL Web.

Lorsque vous utilisez la version par défaut d'un groupe de règles géré, suivez les bonnes pratiques suivantes :

- Abonnez-vous aux notifications : abonnez-vous aux notifications concernant les modifications apportées au groupe de règles et surveillez-les. La plupart des fournisseurs envoient une notification avancée des nouvelles versions statiques et des modifications de version par défaut. Ils vous permettent de vérifier les effets d'une nouvelle version statique avant AWS de passer à la version par défaut. Pour plus d'informations, consultez Être informé des nouvelles versions et mises à jour.
- Passez en revue les effets des paramètres de version statique et apportez les modifications nécessaires avant que votre valeur par défaut ne soit définie sur cette valeur — Avant que votre valeur par défaut ne soit définie sur une nouvelle version statique, examinez les effets de la version statique sur le suivi et la gestion de vos requêtes Web. La nouvelle version statique peut comporter de nouvelles règles à revoir. Recherchez les faux positifs ou tout autre comportement inattendu, au cas où vous auriez besoin de modifier la façon dont vous utilisez le groupe de règles. Vous pouvez définir des règles de comptage, par exemple pour les empêcher de bloquer le trafic pendant que vous déterminez comment vous souhaitez gérer le nouveau comportement. Pour plus d'informations, consultez Tester et ajuster vos AWS WAF protections.

- Version statique : si vous choisissez d'utiliser une version statique, vous devez mettre à jour manuellement le paramètre de version lorsque vous êtes prêt à adopter une nouvelle version du groupe de règles.

  Lorsque vous utilisez une version statique d'un groupe de règles géré, suivez les bonnes pratiques suivantes :

  - Maintenez votre version à jour : veillez à ce que votre groupe de règles géré soit le plus proche possible de la dernière version. Lorsqu'une nouvelle version est publiée, testez-la, ajustez les paramètres selon les besoins et implémentez-la en temps opportun. Pour plus d'informations sur les tests, consultezTester et ajuster vos AWS WAF protections.
  - Abonnement aux notifications : abonnez-vous aux notifications relatives aux modifications apportées au groupe de règles, afin de savoir quand votre fournisseur publie de nouvelles versions statiques. La plupart des fournisseurs notifient à l'avance les modifications de version. En outre, votre fournisseur devra peut-être mettre à jour la version statique que vous utilisez pour combler une faille de sécurité ou pour d'autres raisons urgentes. Vous saurez ce qui se passe si vous êtes abonné aux notifications du fournisseur. Pour plus d'informations, consultez Être informé des nouvelles versions et mises à jour.

- Évitez l'expiration des versions : ne permettez pas à une version statique d'expirer pendant que vous l'utilisez. La gestion des versions expirées par le fournisseur peut varier et peut inclure le fait de forcer une mise à niveau vers une version disponible ou d'autres modifications susceptibles d'avoir des conséquences inattendues. Suivez la métrique AWS WAF d'expiration et définissez une alarme qui vous donne un nombre de jours suffisant pour réussir la mise à niveau vers une version prise en charge. Pour plus d'informations, voir Expiration des versions de suivi.

Utilisation des groupes de règles gérés

Cette section fournit des conseils pour accéder à vos groupes de règles gérés et les gérer.

Lorsque vous ajoutez un groupe de règles géré à votre ACL Web, vous pouvez choisir les mêmes options de configuration que vos propres groupes de règles, ainsi que des paramètres supplémentaires.

La console vous permet d'accéder aux informations des groupes de règles gérés pendant le processus d'ajout et de modification des règles dans vos ACL Web. Par le biais des API et de l'interface de ligne de commande (CLI), vous pouvez directement demander des informations sur les groupes de règles gérés.

Lorsque vous utilisez un groupe de règles géré dans votre ACL Web, vous pouvez modifier les paramètres suivants :

- Version : cette option n'est disponible que si le groupe de règles est versionné. Pour plus d'informations, consultez Groupes de règles gérés versionnés.
- Remplacer les actions des règles : vous pouvez remplacer les actions des règles du groupe de règles par n'importe quelle action. CountIl est utile de les définir sur pour tester un groupe de règles avant de l'utiliser pour gérer vos requêtes Web. Pour plus d'informations, consultez Les actions des règles du groupe de règles remplacent les actions.
- Instruction scope-down : vous pouvez ajouter une instruction scope-down pour filtrer les requêtes Web que vous ne souhaitez pas évaluer avec le groupe de règles. Pour plus d'informations, consultez Déclarations de portée réduite.
- Annuler l'action du groupe de règles : vous pouvez annuler l'action résultant de l'évaluation du groupe de règles et lui attribuer Count la valeur uniquement. Cette option n'est pas couramment utilisée. Cela ne modifie pas la façon dont AWS WAF les règles du groupe de règles sont évaluées.

Pour plus d'informations, consultez L'action de retour du groupe de règles est remplacée par Count.

Pour modifier les paramètres des groupes de règles gérés dans votre ACL Web

- Console
  - (Option) Lorsque vous ajoutez le groupe de règles gérées à votre ACL Web, vous pouvez choisir Modifier pour afficher et modifier les paramètres.
  - (Option) Après avoir ajouté le groupe de règles gérées dans votre ACL Web, sur la page ACL Web, choisissez l'ACL Web que vous venez de créer. Cela vous amène à la page de modification de la liste ACL web.
    - Choisissez Rules (Règles).
    - Sélectionnez le groupe de règles, puis choisissez Modifier pour afficher et modifier les paramètres.
- API et CLI : en dehors de la console, vous pouvez gérer les paramètres du groupe de règles géré lorsque vous créez et mettez à jour l'ACL Web.

Récupération de la liste des groupes de règles gérés

Vous pouvez récupérer la liste des groupes de règles gérés que vous pouvez utiliser dans vos ACL Web. La liste inclut les éléments suivants :

- Tous les groupes de règles de règles AWS gérées.
- Les groupes de AWS Marketplace règles auxquels vous êtes abonné.

> **Note**
>
> Pour plus d'informations sur l'abonnement à des groupes de AWS Marketplace règles, consultezAWS Marketplace groupes de règles gérés.

Lorsque vous récupérez la liste des groupes de règles gérés, la liste que vous obtenez dépend de l'interface que vous utilisez :

- Console : via la console, vous pouvez voir tous les groupes de règles gérés, y compris les groupes de AWS Marketplace règles auxquels vous n'êtes pas encore abonné. Pour ceux auxquels vous n'êtes pas encore abonné, l'interface fournit des liens que vous pouvez suivre pour vous abonner.
- API et CLI : en dehors de la console, votre demande renvoie uniquement les groupes de règles que vous pouvez utiliser.

Pour récupérer la liste des groupes de règles gérés

- Console — Au cours du processus de création d'une ACL Web, sur la page Ajouter des règles et des groupes de règles, choisissez Ajouter des groupes de règles gérés. Au niveau supérieur, les noms des fournisseurs sont répertoriés. Développez la liste de chaque fournisseur pour voir la liste des groupes de règles gérés. Pour les groupes de règles versionnés, les informations affichées à ce niveau concernent la version par défaut. Lorsque vous ajoutez un groupe de règles gérées à votre liste ACL web, la console le répertorie en fonction du schéma d'attribution de noms `<Vendor Name>-<Managed Rule Group Name>`.
- API —
  - `ListAvailableManagedRuleGroups`
- CLI —
  - `aws wafv2 list-available-managed-rule-groups --scope=<CLOUDFRONT|REGIONAL>`

Récupération des règles dans un groupe de règles géré

Vous pouvez récupérer la liste des règles d'un groupe de règles géré. Les appels d'API et de CLI renvoient les spécifications des règles auxquelles vous pouvez faire référence dans le modèle JSON ou via celui-ci AWS CloudFormation.

Pour extraire la liste des règles d'un groupe de règles gérées

- Console
  - (Option) Lorsque vous ajoutez le groupe de règles gérées à votre ACL Web, vous pouvez choisir Modifier pour afficher les règles.
  - (Option) Après avoir ajouté le groupe de règles gérées dans votre ACL Web, sur la page ACL Web, choisissez l'ACL Web que vous venez de créer. Cela vous amène à la page de modification de la liste ACL web.
    - Choisissez Rules (Règles).

    - Sélectionnez le groupe de règles pour lequel vous souhaitez voir une liste de règles, puis choisissez Modifier. AWS WAF affiche la liste des règles du groupe de règles.
- API — `DescribeManagedRuleGroup`
- CLI — `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Extraction des versions disponibles pour un groupe de règles géré

Les versions disponibles d'un groupe de règles géré sont des versions dont l'expiration n'a pas encore été programmée. La liste indique quelle version est la version par défaut actuelle pour le groupe de règles.

Pour récupérer la liste des versions disponibles d'un groupe de règles géré

- Console
    - (Option) Lorsque vous ajoutez le groupe de règles géré à votre ACL Web, choisissez Modifier pour voir les informations du groupe de règles. Développez le menu déroulant Version pour voir la liste des versions disponibles.
    - (Option) Après avoir ajouté le groupe de règles géré à votre ACL Web, choisissez Modifier sur l'ACL Web, puis sélectionnez et modifiez la règle du groupe de règles. Développez le menu déroulant Version pour voir la liste des versions disponibles.
- API —
    - `ListAvailableManagedRuleGroupVersions`
- CLI —
    - `aws wafv2 list-available-managed-rule-group-versions --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Ajout d'un groupe de règles géré à une ACL Web via la console

Ces instructions s'appliquent à tous les groupes de règles AWS Managed Rules et aux groupes de AWS Marketplace règles auxquels vous êtes abonné.

Risque lié au trafic de production

Avant de déployer des modifications dans votre ACL Web pour le trafic de production, testez-les et ajustez-les dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite vos règles mises à jour en mode décompte en fonction de votre trafic de production avant de les activer. Pour de plus amples informations, consultez Tester et ajuster vos AWS WAF protections.

Note

L'utilisation de plus de 1 500 WCU dans une ACL Web entraîne des coûts supérieurs au prix de base de l'ACL Web. Pour plus d'informations, veuillez consulter les sections AWS WAF unités de capacité ACL Web (WCU) et Tarification d'AWS WAF.

Pour ajouter un groupe de règles géré à une ACL Web via la console

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Choisissez les ACL Web dans le volet de navigation.
3. Sur la page ACL Web, dans la liste des ACL Web, sélectionnez celle à laquelle vous souhaitez ajouter le groupe de règles. Cela vous amène à la page de l'ACL Web unique.
4. Sur la page de votre ACL Web, choisissez l'onglet Règles.
5. Dans le volet Règles, choisissez Ajouter des règles, puis Ajouter des groupes de règles gérés.
6. Sur la page Ajouter des groupes de règles gérés, élargissez la sélection de votre fournisseur de groupes de règles pour voir la liste des groupes de règles disponibles.
7. Pour chaque groupe de règles que vous souhaitez ajouter, choisissez Ajouter à l'ACL Web. Si vous souhaitez modifier la configuration de l'ACL Web pour le groupe de règles, choisissez Modifier, apportez vos modifications, puis sélectionnez Enregistrer la règle. Pour plus d'informations sur les options, consultez les instructions de versionnement Groupes de règles gérés versionnés et les instructions d'utilisation d'un groupe de règles géré dans une ACL Web à l'Instruction de groupe de règles géréadresse.
8. Au bas de la page Ajouter des groupes de règles gérés, choisissez Ajouter des règles.

9. Sur la page Définir la priorité des règles, ajustez l'ordre dans lequel les règles s'exécutent selon les besoins, puis choisissez Enregistrer. Pour plus d'informations, consultez Ordre de traitement des règles et des groupes de règles dans une ACL Web.

Sur la page de votre ACL Web, les groupes de règles gérés que vous avez ajoutés sont répertoriés sous l'onglet Règles.

Testez et ajustez les modifications apportées à vos AWS WAF protections avant de les utiliser pour le trafic de production. Pour plus d'informations, consultez Tester et ajuster vos AWS WAF protections.

Incohérences temporaires lors des mises à jour

Lorsque vous créez ou modifiez une ACL Web ou d'autres AWS WAF ressources, les modifications mettent peu de temps à se propager à toutes les zones où les ressources sont stockées. Le temps de propagation peut aller de quelques secondes à plusieurs minutes.

Voici des exemples d'incohérences temporaires que vous pourriez remarquer lors de la propagation des modifications :

- Après avoir créé une ACL Web, si vous essayez de l'associer à une ressource, vous pouvez obtenir une exception indiquant que l'ACL Web n'est pas disponible.
- Une fois que vous avez ajouté un groupe de règles à une ACL Web, les nouvelles règles de groupe de règles peuvent être en vigueur dans une zone où l'ACL Web est utilisée et pas dans une autre.
- Une fois que vous avez modifié le paramètre d'une action de règle, vous pouvez voir l'ancienne action à certains endroits et la nouvelle action à d'autres.
- Après avoir ajouté une adresse IP à un ensemble d'adresses IP utilisé dans une règle de blocage, la nouvelle adresse peut être bloquée dans une zone alors qu'elle est toujours autorisée dans une autre.

Être informé des nouvelles versions et des mises à jour d'un groupe de règles géré

Un fournisseur de groupes de règles gérés utilise les notifications SNS pour annoncer les modifications apportées aux groupes de règles, telles que les nouvelles versions à venir et les mises à jour de sécurité urgentes.

Comment s'abonner aux notifications SNS

Pour vous abonner aux notifications d'un groupe de règles, vous devez créer un abonnement Amazon SNS pour l'ARN de la rubrique Amazon SNS du groupe de règles dans la région us-east-1 des États-Unis (Virginie du Nord).

Pour plus d'informations sur la procédure d'abonnement, consultez le guide du développeur Amazon Simple Notification Service.

> **Note**
>
> Créez votre abonnement au sujet SNS uniquement dans la région us-east-1.

Les groupes de règles AWS gérées versionnés utilisent tous la même rubrique SNS : Amazon Resource Name (ARN). Pour plus d'informations sur les notifications de groupes de règles AWS gérées, consultezNotifications de déploiement.

Où trouver l'ARN de la rubrique Amazon SNS pour un groupe de règles géré

AWS Les groupes de règles gérées utilisent un seul ARN de rubrique SNS. Vous pouvez donc récupérer l'ARN du sujet auprès de l'un des groupes de règles et vous y abonner pour recevoir des notifications pour tous les groupes de règles de règles AWS gérées qui fournissent des notifications SNS.

- Console
  - (Option) Lorsque vous ajoutez le groupe de règles géré à votre ACL Web, choisissez Modifier pour voir les informations du groupe de règles, y compris l'ARN de la rubrique Amazon SNS du groupe de règles.
  - (Option) Après avoir ajouté le groupe de règles géré à votre ACL Web, choisissez Modifier sur l'ACL Web, puis sélectionnez et modifiez la règle du groupe de règles pour voir l'ARN de la rubrique Amazon SNS du groupe de règles.
- API — `DescribeManagedRuleGroup`
- CLI — `aws wafv2 describe-managed-rule-group --scope=<CLOUDFRONT|REGIONAL> --vendor-name <vendor> --name <managedrule_name>`

Pour obtenir des informations générales sur les formats de notification Amazon SNS et sur la manière de filtrer les notifications que vous recevez, consultez la section Analyse des formats de message et politiques de filtrage des abonnements Amazon SNS dans le guide du développeur Amazon Simple Notification Service.

Suivi de l'expiration des versions d'un groupe de règles

Si vous utilisez une version spécifique d'un groupe de règles, assurez-vous de ne pas continuer à utiliser une version au-delà de sa date d'expiration.

> **Tip**
>
> Inscrivez-vous aux notifications Amazon SNS pour les groupes de règles gérés et tenez-vous au courant des versions des groupes de règles gérés. Vous bénéficierez de la plus grande up-to-date protection offerte par le groupe de règles et vous éviterez l'expiration. Pour plus d'informations, veuillez consulter Être informé des nouvelles versions et mises à jour.

Pour surveiller le calendrier d'expiration d'un groupe de règles géré via Amazon CloudWatch

1. Dans CloudWatch, recherchez les mesures d'expiration AWS WAF de votre groupe de règles géré. Les métriques ont les noms et dimensions suivants :
   - Nom de métrique : DaysToExpiry
   - Dimensions métriques : RegionManagedRuleGroup,Vendor, et Version

   Si vous avez un groupe de règles géré dans votre ACL Web qui évalue le trafic, vous obtiendrez une métrique correspondante. La métrique n'est pas disponible pour les groupes de règles que vous n'utilisez pas.
2. Définissez une alarme sur les métriques qui vous intéressent, afin d'être averti à temps pour passer à une version plus récente du groupe de règles.

Pour plus d'informations sur l'utilisation CloudWatch des métriques Amazon et la configuration des alarmes, consultez le guide de CloudWatch l'utilisateur Amazon.

Exemples de configurations de groupes de règles gérés en JSON et YAML

Les appels d'API et de CLI renvoient une liste de toutes les règles du groupe de règles géré auxquelles vous pouvez faire référence dans le modèle JSON ou via celui-ci AWS CloudFormation.

JSON

Vous pouvez référencer et modifier des groupes de règles gérées au sein d'une instruction de règle à l'aide de JSON. La liste suivante montre le groupe de règles AWS

gérées`AWSManagedRulesCommonRuleSet`, au format JSON. La RuleActionOverrides spécification répertorie une règle dont l'action a été remplacée par. 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

Vous pouvez référencer et modifier des groupes de règles gérés dans une déclaration de règle à l'aide du modèle AWS CloudFormation YAML. La liste suivante montre le groupe de règles

AWS géréesAWSManagedRulesCommonRuleSet, dans le AWS CloudFormation modèle. La RuleActionOverrides spécification répertorie une règle dont l'action a été remplacée par. 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 Règles gérées pour AWS WAF

AWS Managed Rules for AWS WAF est un service géré qui fournit une protection contre les vulnérabilités courantes des applications ou contre tout autre trafic indésirable. Vous avez la possibilité de sélectionner un ou plusieurs groupes de règles dans Règles AWS gérées pour chaque ACL Web, jusqu'à la limite maximale d'unités de capacité des ACL Web (WCU).

Atténuer les faux positifs et tester les modifications des groupes de règles

Avant d'utiliser un groupe de règles géré en production, testez-le dans un environnement hors production conformément aux Tester et ajuster vos AWS WAF protections instructions de. Suivez les instructions de test et de réglage lorsque vous ajoutez un groupe de règles à votre ACL Web, pour tester une nouvelle version d'un groupe de règles et chaque fois qu'un groupe de règles ne gère pas votre trafic Web comme vous le souhaitez.

Responsabilités de sécurité partagées

AWS Les règles gérées sont conçues pour vous protéger contre les menaces Web les plus courantes. Lorsqu'ils sont utilisés conformément à la documentation, les groupes de règles AWS gérées ajoutent un niveau de sécurité supplémentaire à vos applications. Cependant, les groupes

de règles AWS gérées ne sont pas destinés à remplacer vos responsabilités en matière de sécurité, qui sont déterminées par les AWS ressources que vous sélectionnez. Reportez-vous au modèle de responsabilité partagée pour vous assurer que vos ressources AWS sont correctement protégées.

AWS Liste des groupes de règles gérées

Les informations que nous publions concernant les règles des groupes de règles AWS gérées sont destinées à vous fournir suffisamment d'informations pour utiliser les règles, sans fournir d'informations que des acteurs malveillants pourraient utiliser pour contourner les règles. Si vous avez besoin de plus d'informations que celles que vous trouverez dans cette documentation, contactez le AWS Support Centre.

Cette section décrit les versions les plus récentes des groupes de règles AWS gérées. Vous les voyez sur la console lorsque vous ajoutez un groupe de règles gérées à votre liste ACL web. Grâce à l'API, vous pouvez récupérer cette liste ainsi que les groupes de règles AWS Marketplace gérés auxquels vous êtes abonné en appelant`ListAvailableManagedRuleGroups`.

> **Note**
>
> Pour plus d'informations sur la récupération des versions d'un groupe de règles AWS gérées, consultezExtraction des versions disponibles pour un groupe de règles géré.

Tous les groupes de règles AWS gérées prennent en charge l'étiquetage, et les listes de règles de cette section incluent les spécifications des étiquettes. Vous pouvez récupérer les étiquettes d'un groupe de règles géré via l'API en appelant`DescribeManagedRuleGroup`. Les étiquettes sont répertoriées dans la AvailableLabels propriété de la réponse. Pour plus d'informations sur l'étiquetage, consultezAWS WAF étiquettes sur les requêtes Web.

Testez et ajustez les modifications apportées à vos AWS WAF protections avant de les utiliser pour le trafic de production. Pour plus d'informations, consultez Tester et ajuster vos AWS WAF protections.

AWS Groupes de règles gérées

- Groupes de règles de référence
  - Groupe de règles géré par un ensemble de règles de base (CRS)
  - Groupe de règles géré par la protection des administrateurs
  - Groupe de règles géré pour les entrées erronées connues
- Groupes de règles spécifiques au cas d'utilisation

Groupes de règles de référence

Les groupes de règles gérées de base offrent une protection générale contre une grande variété de menaces courantes. Choisissez un ou plusieurs de ces groupes de règles pour établir une protection de base pour vos ressources.

> **Note**
>
> Les informations que nous publions concernant les règles des groupes de règles AWS gérées sont destinées à vous fournir suffisamment d'informations pour utiliser les règles, sans fournir d'informations que des acteurs malveillants pourraient utiliser pour contourner les règles. Si vous avez besoin de plus d'informations que celles que vous trouverez dans cette documentation, contactez le AWS Support Centre.

Groupe de règles géré par un ensemble de règles de base (CRS)

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

Le groupe de règles de base (CRS) contient des règles généralement applicables aux applications Web. Cela fournit une protection contre l'exploitation d'un large éventail de vulnérabilités, y compris certaines des vulnérabilités à haut risque et fréquentes décrites dans les publications de l'OWASP telles que le Top 10 de l'OWASP. Envisagez d'utiliser ce groupe de règles pour tous les cas AWS WAF d'utilisation.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques d'Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

> **Note**
>
> Ce tableau décrit la dernière version statique de ce groupe de règles. Pour les autres versions, utilisez la commande API DescribeManagedRuleGroup.

Nom de la règle	Description et étiquette
`NoUserAgent_HEADER`	Vérifie les requêtes pour lesquelles il manque l'`User-Agent` en-tête HTTP. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
`UserAgent_BadBots_HEADER`	Vérifie les valeurs `User-Agent` d'en-tête communes qui indiquent que la demande est un robot défectueux. Les exemples de modèles incluent `nessus` et `nmap`. Pour la gestion des bots, voir également AWS WAF Groupe de règles Bot Control. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:BadBots_Header`
`SizeRestrictions_QUERYSTRING`	Inspecte les chaînes de requête d'URI de plus de 2 048 octets. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:SizeRestrictions_QueryString`
`SizeRestrictions_Cookie_HEADER`	Vérifie la présence d'en-têtes de cookies de plus de 10 240 octets. Action de la règle Block

Nom de la règle	Description et étiquette
	Libellé : `awswaf:managed:aws:core-rule-set:SizeRestrictions_Cookie_Header`
`SizeRestrictions_BODY`	Vérifie les corps de demande dont la taille est supérieure à 8 Ko (8 192 octets). Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:SizeRestrictions_Body`
`SizeRestrictions_URIPATH`	Inspecte les chemins d'URI de plus de 1 024 octets. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:SizeRestrictions_URIPath`

Nom de la règle	Description et étiquette
`EC2MetaDataSSRF_BODY`	Inspecte les tentatives d'exfiltration des métadonnées Amazon EC2 du corps de la demande. **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Body`

Nom de la règle	Description et étiquette
`EC2MetaDataSSRF_COOKIE`	Détecte les tentatives d'exfiltration des métadonnées Amazon EC2 du cookie de demande. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_Cookie`
`EC2MetaDataSSRF_URIPATH`	Inspecte les tentatives d'exfiltration des métadonnées Amazon EC2 depuis le chemin de l'URI de la demande. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_URIPath`
`EC2MetaDataSSRF_QUERYARGUMENTS`	Inspecte les tentatives d'exfiltration des métadonnées Amazon EC2 à partir des arguments de requête. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:EC2MetaDataSSRF_QueryArguments`

Nom de la règle	Description et étiquette
`GenericLFI_QUERYARGUMENTS`	Inspecte la présence d'exploits LFI (Local File Inclusion) dans les arguments de la demande. Les exemples incluent les tentatives de traversée de chemin en utilisant des techniques comme `../../`. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:GenericLFI_QueryArguments`
`GenericLFI_URIPATH`	Inspecte la présence d'exploits LFI (Local File Inclusion) dans le chemin d'URI. Les exemples incluent les tentatives de traversée de chemin en utilisant des techniques comme `../../`. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:GenericLFI_URIPath`

Nom de la règle	Description et étiquette
`GenericLFI_BODY`	Inspecte la présence d'exploits LFI (Local File Inclusion) dans le corps de la demande. Les exemples incluent les tentatives de traversée de chemin en utilisant des techniques comme `../../`. **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:GenericLFI_Body`

Nom de la règle	Description et étiquette
`RestrictedExtensions_URIPATH`	Vérifie les demandes dont les chemins d'URI contiennent des extensions de fichiers système dont la lecture ou l'exécution ne sont pas sûres. Les exemples de modèles incluent des extensions comme `.log` et `.ini`. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:RestrictedExtensions_URIPath`
`RestrictedExtensions_QUERYARGUMENTS`	Vérifie les demandes dont les arguments de requête contiennent des extensions de fichiers système dont la lecture ou l'exécution ne sont pas sûres. Les exemples de modèles incluent des extensions comme `.log` et `.ini`. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:RestrictedExtensions_QueryArguments`

Nom de la règle	Description et étiquette
`GenericRFI_QUERYARGUMENTS`	Inspecte les valeurs de tous les paramètres de requête pour détecter les tentatives d'exploitation de RFI (Remote File Inclusion) dans les applications Web en incorporant des URL contenant des adresses IPv4. Les exemples incluent des modèles tels que `http://`, `https://`, `ftp://`, `ftps://`, et `file://`, avec un en-tête d'hôte IPv4 dans la tentative d'exploitation. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:GenericRFI_QueryArguments`

Nom de la règle	Description et étiquette
`GenericRFI_BODY`	Inspecte le corps de la demande pour détecter toute tentative d'exploitation de RFI (Remote File Inclusion) dans les applications Web en incorporant des URL contenant des adresses IPv4. Les exemples incluent des modèles tels que `http://`,`https://`,`ftp://`,`ftps://`, et`file://`, avec un en-tête d'hôte IPv4 dans la tentative d'exploitation. **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:GenericRFI_Body`

Nom de la règle	Description et étiquette
`GenericRFI_URIPATH`	Inspecte le chemin de l'URI pour détecter les tentatives d'exploitation de RFI (Remote File Inclusion) dans les applications Web en incorporant des URL contenant des adresses IPv4. Les exemples incluent des modèles tels que `http://`,`https://`,`ftp://`,`ftps://`, et`file://`, avec un en-tête d'hôte IPv4 dans la tentative d'exploitation. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:GenericRFI_URIPath`
`CrossSiteScripting_COOKIE`	Inspecte les valeurs des en-têtes de cookies pour détecter les modèles courants de script intersite (XSS) à l'aide de la fonction intégrée. AWS WAF Instruction d'attaque par scripts inter-site de règle Les exemples de modèles incluent des scripts comme `<script>alert("hello")</script>` . **Note** Les détails de correspondance des règles dans les AWS WAF journaux ne sont pas renseignés pour la version 2.0 de ce groupe de règles. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Cookie`

Nom de la règle	Description et étiquette
`CrossSiteScripting_QUERYARGUMENTS`	Inspecte les valeurs des arguments de requête pour détecter les modèles de script intersite (XSS) courants à l'aide de la fonction intégrée. AWS WAF Instruction d'attaque par scripts inter-site de règle Les exemples de modèles incluent des scripts comme `<script>alert("hello")</script>` . **Note** Les détails de correspondance des règles dans les AWS WAF journaux ne sont pas renseignés pour la version 2.0 de ce groupe de règles. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:CrossSiteScripting_QueryArguments`

Nom de la règle	Description et étiquette
`CrossSiteScripting_BODY`	Inspecte le corps de la requête à la recherche de modèles de script intersite (XSS) courants à l'aide de la fonction intégrée. AWS WAF Instruction d'attaque par scripts inter-site de règle Les exemples de modèles incluent des scripts comme `<script>alert("hello")</script>` . **Note** Les détails de correspondance des règles dans les AWS WAF journaux ne sont pas renseignés pour la version 2.0 de ce groupe de règles. **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des

Nom de la règle	Description et étiquette
	composants de demande surdimens ionnés dans AWS WAF. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:CrossSiteScripting_Body`
`CrossSiteScripting_URIPATH`	Inspecte la valeur du chemin d'URI pour détecter les modèles de script intersite (XSS) courants à l'aide de la fonction intégrée. AWS WAF Instruction d'attaque par scripts inter-site de règle Les exemples de modèles incluent des scripts comme `<script>alert("hello")</script>` . **Note** Les détails de correspondance des règles dans les AWS WAF journaux ne sont pas renseignés pour la version 2.0 de ce groupe de règles. Action de la règle Block Libellé : `awswaf:managed:aws:core-rule-set:CrossSiteScripting_URIPath`

Groupe de règles géré par la protection des administrateurs

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

Le groupe de règles Protection administrateur contient des règles qui vous permettent de bloquer l'accès externe aux pages administratives exposées. Cela peut être utile si vous exécutez un logiciel tiers ou si vous souhaitez réduire le risque qu'un acteur malveillant accède à votre application comme administrateur.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques d'Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

> **Note**
>
> Ce tableau décrit la dernière version statique de ce groupe de règles. Pour les autres versions, utilisez la commande API DescribeManagedRuleGroup.

Nom de la règle	Description et étiquette
`AdminProtection_URIPATH`	Inspecte les chemins d'URI qui sont généralement réservés à l'administration d'un serveur Web ou d'une application. Les exemples de modèles incluent `sqlmanager` . Action de la règle Block Libellé : `awswaf:managed:aws:admin-protection:AdminProtection_URIPath`

Groupe de règles géré pour les entrées erronées connues

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

Le groupe de règles Known Bad Inputs (Entrées défectueuses connues) contient des règles permettant de bloquer les modèles de demande connus comme non valides et associés à

l'exploitation ou à la découverte de vulnérabilités. Cela peut aider à réduire le risque qu'un acteur malveillant ne découvre une application vulnérable.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques d'Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

> **Note**
>
> Ce tableau décrit la dernière version statique de ce groupe de règles. Pour les autres versions, utilisez la commande API DescribeManagedRuleGroup.

Nom de la règle	Description et étiquette
`JavaDeserializationRCE_HEADER`	Inspecte les clés et les valeurs des en-têtes de requêtes HTTP pour détecter des modèles indiquant des tentatives d'exécution de commandes à distance (RCE) de Java, tels que les vulnérabilités Spring Core et Cloud Function RCE (CVE-22963, CVE-22965). Les exemples de modèles incluent `(java.lang.Runtime ).getRuntime().exec("whoami")` . **Warning** Cette règle inspecte uniquement les 8 premiers Ko des en-têtes de demande ou les 200 premiers en-têtes, selon la première limite atteinte, et utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des

Nom de la règle	Description et étiquette
	composants de demande surdimens ionnés dans AWS WAF. Action de la règle Block Libellé : `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Header`

Nom de la règle	Description et étiquette
`JavaDeserializationRCE_BODY`	Inspecte le corps de la demande pour détecter des modèles indiquant des tentatives d'exécution de commandes à distance (RCE) de Java, tels que les vulnérabilités Spring Core et Cloud Function RCE (CVE-22963, CVE-22965). Les exemples de modèles incluent `(java.lang.Runtime).getRuntime().exec("whoami")` . **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Libellé : `awswaf:managed:aws:known-bad-inputs:JavaDeserializationRCE_Body`

Nom de la règle	Description et étiquette
`JavaDeserializationRCE_URIPATH`	Inspecte l'URI de la demande pour détecter des modèles indiquant des tentatives d'exécution de commandes à distance (RCE) de désériali sation en Java, tels que les vulnérabilités Spring Core et Cloud Function RCE (CVE-2296 3, CVE-22965). Les exemples de modèles incluent `(java.lang.Runtime).getRunt ime().exec("whoami")` . Action de la règle Block Libellé : `awswaf:managed:aws:known- bad-inputs:JavaDeserializatio nRCE_URIPath`
`JavaDeserializationRCE_QUER YSTRING`	Inspecte la chaîne de requête à la recherche de modèles indiquant des tentatives d'exécuti on à distance (RCE) de désérialisation en Java, tels que les vulnérabilités Spring Core et Cloud Function RCE (CVE-22963, CVE-22965). Les exemples de modèles incluent `(java.lan g.Runtime).getRuntime().exe c("whoami")` . Action de la règle Block Libellé : `awswaf:managed:aws:known- bad-inputs:JavaDeserializatio nRCE_QueryString`

Nom de la règle	Description et étiquette
`Host_localhost_HEADER`	Inspecte l'en-tête de l'hôte dans la demande pour les modèles indiquant localhost. Les exemples de modèles incluent `localhost` . Action de la règle Block Libellé : `awswaf:managed:aws:known-bad-inputs:Host_Localhost_Header`
`PROPFIND_METHOD`	Inspecte la méthode HTTP dans la requête pour `PROPFIND`, qui est une méthode similaire à `HEAD`, mais avec l'intention supplémentaire d'exfiltrer des objets XML. Action de la règle Block Libellé : `awswaf:managed:aws:known-bad-inputs:Propfind_Method`
`ExploitablePaths_URIPATH`	Inspecte le chemin URI pour les tentatives d'accès aux chemins d'application Web exploitables. Les exemples de modèles incluent des chemins comme `web-inf`. Action de la règle Block Libellé : `awswaf:managed:aws:known-bad-inputs:ExploitablePaths_URIPath`

Nom de la règle	Description et étiquette
`Log4JRCE_HEADER`	Inspecte les clés et les valeurs des en-têtes de requête pour détecter la présence de la vulnérabilité Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) et protège contre les tentatives d'exécution de code à distance (RCE). Les exemples de modèles incluent `${jndi:ldap://example.com/}` . **Warning** Cette règle inspecte uniquement les 8 premiers Ko des en-têtes de demande ou les 200 premiers en-têtes, selon la première limite atteinte, et utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Libellé : `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Header`

Nom de la règle	Description et étiquette
`Log4JRCE_QUERYSTRING`	Inspecte la chaîne de requête pour détecter la présence de la vulnérabilité Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) et protège contre les tentatives d'exécution de code à distance (RCE). Les exemples de modèles incluent `${jndi:ldap://example.com/}` . Action de la règle Block Libellé : `awswaf:managed:aws:known-bad-inputs:Log4JRCE_QueryString`

Nom de la règle	Description et étiquette
`Log4JRCE_BODY`	Inspecte le corps pour détecter la présence de la vulnérabilité Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) et protège contre les tentatives d'exécution de code à distance (RCE). Les exemples de modèles incluent `${jndi:ldap://example.com/}` . **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Libellé : `awswaf:managed:aws:known-bad-inputs:Log4JRCE_Body`

Nom de la règle	Description et étiquette
`Log4JRCE_URIPATH`	Inspecte le chemin de l'URI pour détecter la présence de la vulnérabilité Log4j (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105) et protège contre les tentatives d'exécution de code à distance (RCE). Les exemples de modèles incluent `${jndi:ldap://example.com/}` . Action de la règle Block Libellé : `awswaf:managed:aws:known-bad-inputs:Log4JRCE_URIPath`

Groupes de règles spécifiques au cas d'utilisation

Les groupes de règles spécifiques aux cas d'utilisation fournissent une protection incrémentielle pour de nombreux cas d'utilisation différents AWS WAF . Choisissez les groupes de règles qui s'appliquent à votre application.

> **Note**
>
> Les informations que nous publions concernant les règles des groupes de règles AWS gérées sont destinées à vous fournir suffisamment d'informations pour utiliser les règles, sans fournir d'informations que des acteurs malveillants pourraient utiliser pour contourner les règles. Si vous avez besoin de plus d'informations que celles que vous trouverez dans cette documentation, contactez le AWS Support Centre.

Groupe de règles géré par base de données SQL

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

Le groupe de règles Base de données SQL contient des règles pour bloquer les modèles de demande associés à l'exploitation des bases de données SQL, comme les attaques par injection SQL. Cela peut aider à empêcher l'injection à distance de requêtes non autorisées. Évaluez ce groupe de règles pour l'utiliser si votre application s'interface avec une base de données SQL.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

> **Note**
>
> Ce tableau décrit la dernière version statique de ce groupe de règles. Pour les autres versions, utilisez la commande API DescribeManagedRuleGroup.

Nom de la règle	Description et étiquette
`SQLi_QUERYARGUMENTS`	Utilise le paramètre intégré AWS WAF Instruction d'attaque par injection SQL de règle, avec un niveau de sensibilité défini surLow, pour inspecter les valeurs de tous les paramètres de requête afin de détecter des modèles correspondant à du code SQL malveillant. Action de la règle Block Étiquette : `awswaf:managed:aws:sql-database:SQLi_QueryArguments`
`SQLiExtendedPatterns_QUERYARGUMENTS`	Inspecte les valeurs de tous les paramètres de la demande pour les modèles qui correspondent au code SQL malveillant. Les modèles détectés par cette règle ne sont pas couverts par la règle`SQLi_QUERYARGUMENTS` . Action de la règle Block Étiquette : `awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments`

Nom de la règle	Description et étiquette
`SQLi_BODY`	Utilise le paramètre intégré AWS WAF Instruction d'attaque par injection SQL de règle, avec un niveau de sensibilité défini surLow, pour inspecter le corps de la demande afin de détecter des modèles correspondant à du code SQL malveillant. **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Étiquette : `awswaf:managed:aws:sql-database:SQLi_Body`

Nom de la règle	Description et étiquette
`SQLiExtendedPatterns_BODY`	Inspecte le corps de la demande pour détecter les modèles correspondant à du code SQL malveillant. Les modèles détectés par cette règle ne sont pas couverts par la règle`SQLi_BODY` . **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Étiquette : `awswaf:managed:aws:sql-database:SQLiExtendedPatterns_Body`

Nom de la règle	Description et étiquette
`SQLi_COOKIE`	Utilise le paramètre intégré AWS WAF Instruction d'attaque par injection SQL de règle, avec un niveau de sensibilité défini surLow, pour inspecter les en-têtes des cookies de demande afin de détecter des modèles correspondant à du code SQL malveillant. Action de la règle Block Étiquette : `awswaf:managed:aws:sql-database:SQLi_Cookie`

Groupe de règles géré par le système d'exploitation Linux

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

Le groupe de règles du système d'exploitation Linux contient des règles qui bloquent les modèles de demande associés à l'exploitation de vulnérabilités spécifiques à Linux, y compris les attaques LFI (Local File Inclusion) propres à Linux. Cela peut aider à prévenir les attaques qui exposent le contenu des fichiers ou exécutent du code auquel l'attaquant n'aurait pas dû avoir accès. Vous devez évaluer ce groupe de règles si une partie de votre application s'exécute sous Linux. Vous devez utiliser ce groupe de règles conjointement avec le groupe de règles Système d'exploitation POSIX.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

> **Note**
>
> Ce tableau décrit la dernière version statique de ce groupe de règles. Pour les autres versions, utilisez la commande API DescribeManagedRuleGroup.

Nom de la règle	Description et étiquette
`LFI_URIPATH`	Inspecte le chemin de la demane pour les tentatives d'exploitation des vulnérabilités LFI (Local File Inclusion) dans les applicati ons Web. Les exemples de modèles incluent des fichiers comme `/proc/version` , qui pourraient fournir des informations sur le système d'exploitation aux attaquants. Action de la règle Block Étiquette : `awswaf:managed:aws:linux-os:LFI_URIPath`
`LFI_QUERYSTRING`	Inspecte les valeurs de la chaîne de requête pour détecter les tentatives d'exploitation des vulnérabilités d'inclusion de fichiers locaux (LFI) dans les applications Web. Les exemples de modèles incluent des fichiers comme `/proc/version` , qui pourraient fournir des informati ons sur le système d'exploitation aux attaquant s. Action de la règle Block Étiquette : `awswaf:managed:aws:linux-os:LFI_QueryString`
`LFI_HEADER`	Inspecte les en-têtes des demandes pour détecter toute tentative d'exploitation des vulnérabilités d'inclusion de fichiers locaux (LFI) dans les applications Web. Les exemples de modèles incluent des fichiers comme `/proc/version` , qui pourraient fournir des informati

Nom de la règle	Description et étiquette
	ons sur le système d'exploitation aux attaquant s. ⚠ Warning Cette règle inspecte uniquement les 8 premiers Ko des en-têtes de demande ou les 200 premiers en-têtes, selon la première limite atteinte, et utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Étiquette : `awswaf:managed:aws:linux-os:LFI_Header`

Groupe de règles géré par le système d'exploitation POSIX

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

Le groupe de règles Système d'exploitation POSIX contient des règles qui bloquent les modèles de demande associés à l'exploitation de vulnérabilités spécifiques aux systèmes d'exploitation POSIX et apparentés, y compris les attaques LFI (Local File Inclusion). Cela peut aider à prévenir les attaques qui exposent le contenu des fichiers ou exécutent du code auquel l'attaquant n'aurait pas dû avoir accès. Vous devez évaluer ce groupe de règles si une partie de votre application s'exécute sur un système d'exploitation POSIX ou apparenté, y compris Linux, AIX, HP-UX, macOS, Solaris, FreeBSD, OpenBSD et bien d'autres.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre

également les étiquettes selon les CloudWatch statistiques Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

> **Note**
>
> Ce tableau décrit la dernière version statique de ce groupe de règles. Pour les autres versions, utilisez la commande API DescribeManagedRuleGroup.

Nom de la règle	Description et étiquette
`UNIXShellCommandsVariables_QUERYSTRING`	Inspecte les valeurs de la chaîne de requête pour détecter toute tentative d'exploitation des vulnérabilités liées à l'injection de commandes , au LFI et à la traversée de chemins dans les applications Web exécutées sur des systèmes Unix. Les exemples incluent des modèles comme `echo $HOME` et `echo $PATH` . Action de la règle Block Étiquette : `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString`
`UNIXShellCommandsVariables_BODY`	Inspecte le corps de la requête pour les tentatives d'exploitation des vulnérabilités d'injection de commandes, de LFI et de traversée de chemin dans les applications Web qui s'exécutent sur des systèmes Unix. Les exemples incluent des modèles comme `echo $HOME` et `echo $PATH`.

Nom de la règle	Description et étiquette
	Warning Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Étiquette : `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Body`

Nom de la règle	Description et étiquette
`UNIXShellCommandsVariables_HEADER`	Inspecte tous les en-têtes de demandes pour détecter toute tentative d'exploitation des vulnérabilités liées à l'injection de commandes , au LFI et à la traversée de chemins dans les applications Web exécutées sur des systèmes Unix. Les exemples incluent des modèles comme `echo $HOME` et `echo $PATH`. **Warning** Cette règle inspecte uniquement les 8 premiers Ko des en-têtes de demande ou les 200 premiers en-têtes, selon la première limite atteinte, et utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Étiquette : `awswaf:managed:aws:posix-os:UNIXShellCommandsVariables_Header`

Groupe de règles géré par le système d'exploitation Windows

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

Le groupe de règles du système d'exploitation Windows contient des règles qui bloquent les modèles de demandes associés à l'exploitation de vulnérabilités spécifiques à Windows, telles que l'exécution à distance de PowerShell commandes. Cela permet d'empêcher l'exploitation de vulnérabilités

qui permettent à un attaquant d'exécuter des commandes non autorisées ou d'exécuter du code malveillant. Évaluez ce groupe de règles si une partie de votre application s'exécute sur un système d'exploitation Windows.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

> **Note**
>
> Ce tableau décrit la dernière version statique de ce groupe de règles. Pour les autres versions, utilisez la commande API DescribeManagedRuleGroup.

Nom de la règle	Description et étiquette
`WindowsShellCommands_COOKIE`	Inspecte les en-têtes des cookies de demande pour détecter les tentatives d'injection de WindowsShell commandes dans les applicati ons Web. Les modèles de correspondance représentent des WindowsShell commandes. Les exemples de modèles incluent `||nslooku p  et;cmd`. Action de la règle Block Étiquette : `awswaf:managed:aws :windows-os:WindowsShellCom mands_Cookie`
`WindowsShellCommands_QUERYA RGUMENTS`	Inspecte les valeurs de tous les paramètre s de requête pour détecter les tentatives d'injection de WindowsShell commandes dans les applications Web. Les modèles de correspondance représentent des WindowsSh

Nom de la règle	Description et étiquette
	ell commandes. Les exemples de modèles incluent `||nslookup` et `;cmd`. Action de la règle Block Étiquette : `awswaf:managed:aws:windows-os:WindowsShellCommands_QueryArguments`

Nom de la règle	Description et étiquette
`WindowsShellCommands_BODY`	Inspecte le corps de la requête pour détecter les tentatives d'injection de WindowsShell commandes dans les applications Web. Les modèles de correspondance représentent des WindowsShell commandes. Les exemples de modèles incluent `||nslookup` et `;cmd`. **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Étiquette : `awswaf:managed:aws:windows-os:WindowsShellCommands_Body`

Nom de la règle	Description et étiquette
`PowerShellCommands_COOKIE`	Inspecte les en-têtes des cookies de demande pour détecter les tentatives d'injection de PowerShell commandes dans les applicati ons Web. Les modèles de correspondance représentent des PowerShell commandes. Par exemple, `Invoke-Expression` . Action de la règle Block Étiquette : `awswaf:managed:aws :windows-os:PowerShellComma nds_Cookie`
`PowerShellCommands_QUERYARG UMENTS`	Inspecte les valeurs de tous les paramètres de requête pour détecter les tentatives d'injection de PowerShell commandes dans les applicati ons Web. Les modèles de correspondance représentent des PowerShell commandes. Par exemple, `Invoke-Expression` . Action de la règle Block Étiquette : `awswaf:managed:aws :windows-os:PowerShellComma nds_QueryArguments`

Nom de la règle	Description et étiquette
`PowerShellCommands_BODY`	Inspecte le corps de la requête pour détecter les tentatives d'injection de PowerShell commandes dans les applications Web. Les modèles de correspondance représentent des PowerShell commandes. Par exemple, `Invoke-Expression` . **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Étiquette : `awswaf:managed:aws:windows-os:PowerShellCommands_Body`

Groupe de règles géré par une application PHP

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

Le groupe de règles Application PHP contient des règles qui bloquent les modèles de demande associés à l'exploitation de vulnérabilités spécifiques à l'utilisation du langage de programmation PHP, y compris l'injection de fonctions PHP dangereuses. Cela permet d'empêcher l'exploitation de vulnérabilités qui permettent à un attaquant d'exécuter à distance du code ou des commandes pour lesquels il n'est pas autorisé. Évaluez ce groupe de règles si PHP est installé sur un serveur avec lequel votre application s'interface.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

> **Note**
>
> Ce tableau décrit la dernière version statique de ce groupe de règles. Pour les autres versions, utilisez la commande API DescribeManagedRuleGroup.

Nom de la règle	Description et étiquette
`PHPHighRiskMethodsVariables_HEADER`	Inspecte tous les en-têtes pour détecter les tentatives d'injection de code de script PHP. Les exemples de modèles incluent des fonctions comme `fsockopen` et la variable `$_GET` superglobale. **Warning** Cette règle inspecte uniquement les 8 premiers Ko des en-têtes de demande ou les 200 premiers en-têtes, selon la première limite atteinte, et utilise l'`Continue`option de gestion du

Nom de la règle	Description et étiquette
	contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Étiquette : `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Header`
`PHPHighRiskMethodsVariables_QUERYSTRING`	Inspecte tout ce qui se trouve après le premier élément ? de l'URL de requête, à la recherche de tentatives d'injection de code dans un script PHP. Les exemples de modèles incluent des fonctions comme `fsockopen` et la variable `$_GET` superglobale. Action de la règle Block Étiquette : `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_QueryString`

Nom de la règle	Description et étiquette
`PHPHighRiskMethodsVariables_BODY`	Inspecte les valeurs du corps de la demande pour les tentatives d'injection de code PHP. Les exemples de modèles incluent des fonctions comme `fsockopen` et la variable `$_GET` superglobale. **Warning** Cette règle inspecte uniquement le corps de la demande jusqu'à la limite de taille limite pour l'ACL Web et le type de ressource. Pour Application Load Balancer et AWS AppSync, la limite est fixée à 8 Ko. Pour CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access, la limite par défaut est de 16 Ko et vous pouvez l'augmenter jusqu'à 64 Ko dans votre configuration ACL Web. Cette règle utilise l'`Continue`option de gestion du contenu surdimensionné. Pour plus d'informations, consultez Gestion des composants de demande surdimensionnés dans AWS WAF. Action de la règle Block Étiquette : `awswaf:managed:aws:php-app:PHPHighRiskMethodsVariables_Body`

WordPress groupe de règles géré par les applications

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

Le groupe de règles d' WordPress application contient des règles qui bloquent les modèles de demandes associés à l'exploitation de vulnérabilités spécifiques aux WordPress sites. Vous devez évaluer ce groupe de règles si vous courezWordPress. Ce groupe de règles doit être utilisé conjointement avec les groupes de règles Base de données SQL et Application PHP.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

> **Note**
>
> Ce tableau décrit la dernière version statique de ce groupe de règles. Pour les autres versions, utilisez la commande API DescribeManagedRuleGroup.

Nom de la règle	Description et étiquette
`WordPressExploitableCommands_QUERYSTRING`	Inspecte la chaîne de requête pour détecter les WordPress commandes à haut risque susceptibles d'être exploitées dans des installations ou des plugins vulnérables. Les exemples de modèles incluent des commandes comme `do-reset-wordpress` . Action de la règle Block Étiquette : `awswaf:managed:aws:wordpress-app:WordPressExploitableCommands_QUERYSTRING`
`WordPressExploitablePaths_URIPATH`	

Nom de la règle	Description et étiquette
	Inspecte le chemin de l'URI de la demande pour détecter WordPress des fichiers tels que`xmlrpc.php` , connus pour présenter des vulnérabilités facilement exploitables. Action de la règle Block Étiquette : `awswaf:managed:aws:wordpress-app:WordPressExploitablePaths_URIPATH`

Groupes de règles de réputation IP

Les groupes de règles de réputation IP bloquent les demandes en fonction de leur adresse IP source.

> **Note**
>
> Ces règles utilisent l'adresse IP source à partir de l'origine de la requête Web. Si le trafic passe par un ou plusieurs proxys ou équilibreurs de charge, l'origine de la requête Web contiendra l'adresse du dernier proxy, et non l'adresse d'origine du client.

Choisissez un ou plusieurs de ces groupes de règles si vous souhaitez réduire votre exposition au trafic de robot, aux tentatives d'exploitation ou si vous appliquez des restrictions géographiques à votre contenu. Pour la gestion des bots, voir égalementAWS WAF Groupe de règles Bot Control.

Les groupes de règles de cette catégorie ne fournissent pas de notifications de version ni de mise à jour SNS.

> **Note**
>
> Les informations que nous publions concernant les règles des groupes de règles AWS gérées sont destinées à vous fournir suffisamment d'informations pour utiliser les règles, sans fournir d'informations que des acteurs malveillants pourraient utiliser pour contourner les règles. Si vous avez besoin de plus d'informations que celles que vous trouverez dans cette documentation, contactez le AWS Support Centre.

Groupe de règles géré par Amazon IP Reputation

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

Le groupe de règles de la liste de réputation IP Amazon contient des règles basées sur les renseignements internes sur les menaces Amazon. Ceci est utile si vous souhaitez bloquer les adresses IP généralement associées à des robots ou à d'autres menaces. Le blocage de ces adresses IP peut aider à atténuer les robots et à réduire le risque qu'un acteur malveillant ne découvre une application vulnérable.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques d'Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

Nom de la règle	Description et étiquette
`AWSManagedIPReputationList`	Inspecte les adresses IP identifiées comme participant activement à des activités malveillantes. AWS WAF collecte la liste d'adresses IP auprès de diverses sources MadPot, notamment d'un outil de renseignement sur les menaces utilisé par Amazon pour protéger ses clients contre la cybercriminalité. Pour plus d'informations sur MadPot, voirhttps://www.aboutamazon.com/news/aws/amazon-madpot-stops-cybersecurity-crime. Action de la règle Block Libellé : `awswaf:managed:aws:amazon-ip-list:AWSManagedIPReputationList`
`AWSManagedReconnaissanceList`	Inspecte les connexions provenant d'adresses IP qui effectuent une reconnaissance par rapport aux AWS ressources.

Nom de la règle	Description et étiquette
	Action de la règle Block Libellé : `awswaf:managed:aws:amazon-ip-list:AWSManagedReconnaissanceList`
`AWSManagedIPDDoSList`	Inspecte les adresses IP qui ont été identifiées comme participant activement à des activités DDoS. Action de la règle Count Libellé : `awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList`

Groupe de règles géré par liste d'adresses IP anonyme

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

Le groupe de règles de liste d'adresses IP anonymes contient des règles visant à bloquer les demandes provenant de services qui permettent de masquer l'identité du téléspectateur. Il s'agit notamment des demandes des VPN, des proxys, des nœuds Tor et des fournisseurs d'hébergement Web. Ce groupe de règles est utile si vous souhaitez filtrer les utilisateurs qui tentent de masquer leur identité auprès de votre application. Le blocage des adresses IP liées à ces services peut contribuer à limiter les robots et le non-respect des restrictions géographiques.

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques d'Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

Nom de la règle	Description et étiquette
`AnonymousIPList`	Inspecte la liste des adresses IP des sources connues pour anonymiser les informations

Nom de la règle	Description et étiquette
	client, telles que les nœuds TOR, les proxys temporaires et d'autres services de masquage. Action de la règle Block Libellé : `awswaf:managed:aws:anonymous-ip-list:AnonymousIPList`
`HostingProviderIPList`	Recherche une liste d'adresses IP provenant de fournisseurs d'hébergement Web et de cloud, qui sont moins susceptibles de générer du trafic pour les utilisateurs finaux. La liste IP n'inclut pas les adresses AWS IP. Action de la règle Block Libellé : `awswaf:managed:aws:anonymous-ip-list:HostingProviderIPList`

AWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes

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

L'ACFP (AWS WAF Fraud Control Account Creation Fraud Prevention) gère les étiquettes des groupes de règles et gère les demandes susceptibles de faire partie de tentatives de création de compte frauduleuses. Pour ce faire, le groupe de règles inspecte les demandes de création de compte que les clients envoient aux points de terminaison d'enregistrement et de création de compte de votre application.

Le groupe de règles ACFP inspecte les tentatives de création de comptes de différentes manières, afin de vous donner de la visibilité et de contrôler les interactions potentiellement malveillantes. Le groupe de règles utilise des jetons de demande pour recueillir des informations sur le navigateur du client et sur le niveau d'interactivité humaine lors de la création de la demande de création de compte. Le groupe de règles détecte et gère les tentatives de création de comptes en masse en agrégeant les demandes par adresse IP et par session client, et en les agrégeant selon les informations de compte fournies, telles que l'adresse physique et le numéro de téléphone. En outre,

le groupe de règles détecte et bloque la création de nouveaux comptes à l'aide d'informations d'identification compromises, ce qui contribue à protéger le niveau de sécurité de votre application et de vos nouveaux utilisateurs.

Considérations relatives à l'utilisation de ce groupe de règles

Ce groupe de règles nécessite une configuration personnalisée, qui inclut la spécification des chemins d'enregistrement et de création de compte de votre application. Sauf indication contraire, les règles de ce groupe de règles inspectent toutes les demandes que vos clients envoient à ces deux points de terminaison. Pour configurer et implémenter ce groupe de règles, consultez les instructions à l'adresseAWS WAF Contrôle des fraudes : création de comptes, prévention des fraudes (ACFP).

> **Note**
>
> Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d'informations, consultez Tarification d'AWS WAF.

Ce groupe de règles fait partie des protections intelligentes d'atténuation des menaces contenues dans AWS WAF. Pour plus d'informations, veuillez consulter AWS WAF Atténuation intelligente des menaces.

Pour réduire vos coûts et être sûr de gérer votre trafic Web comme vous le souhaitez, utilisez ce groupe de règles conformément aux instructions deMeilleures pratiques pour une atténuation intelligente des menaces.

Ce groupe de règles n'est pas disponible pour les groupes d'utilisateurs Amazon Cognito. Vous ne pouvez pas associer une ACL Web qui utilise ce groupe de règles à un groupe d'utilisateurs, ni ajouter ce groupe de règles à une ACL Web déjà associée à un groupe d'utilisateurs.

Étiquettes ajoutées par ce groupe de règles

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques d'Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

Étiquettes à jetons

Ce groupe de règles utilise la gestion des AWS WAF jetons pour inspecter et étiqueter les requêtes Web en fonction de l'état de leurs AWS WAF jetons. AWS WAF utilise des jetons pour le suivi et la vérification des sessions client.

Pour plus d'informations sur les jetons et leur gestion, consultezAWS WAF jetons de demande Web.

Pour plus d'informations sur les composants de l'étiquette décrits ici, voirAWS WAF syntaxe des étiquettes et exigences de dénomination.

Libellé de session client

L'étiquette `awswaf:managed:token:id:`*`identifier`* contient un identifiant unique que la gestion des AWS WAF jetons utilise pour identifier la session client. L'identifiant peut changer si le client acquiert un nouveau jeton, par exemple après avoir supprimé le jeton qu'il utilisait.

> **Note**
>
> AWS WAF ne communique pas CloudWatch les statistiques Amazon pour cette étiquette.

Étiquettes d'état des jetons : préfixes d'espace de noms d'étiquettes

Les étiquettes d'état du jeton indiquent le statut du jeton ainsi que les informations relatives au défi et au CAPTCHA qu'il contient.

Chaque étiquette de statut de jeton commence par l'un des préfixes d'espace de noms suivants :

- `awswaf:managed:token:`— Utilisé pour signaler l'état général du jeton et pour rendre compte de l'état des informations de défi du jeton.
- `awswaf:managed:captcha:`— Utilisé pour rendre compte de l'état des informations CAPTCHA du jeton.

Étiquettes d'état des jetons : noms des étiquettes

Après le préfixe, le reste de l'étiquette fournit des informations détaillées sur l'état du jeton :

- `accepted`— Le jeton de demande est présent et contient les éléments suivants :

- Un défi ou une solution CAPTCHA valide.
- Un défi ou un horodatage CAPTCHA non expiré.
- Spécification de domaine valide pour l'ACL Web.

Exemple : L'étiquette `awswaf:managed:token:accepted` indique que le jeton des requêtes Web contient une solution de défi valide, un horodatage de défi non expiré et un domaine valide.

- `rejected`— Le jeton de demande est présent mais ne répond pas aux critères d'acceptation.

  Outre l'étiquette rejetée, la gestion des jetons ajoute un espace de noms et un nom d'étiquette personnalisés pour en indiquer la raison.

  - `rejected:not_solved`— Le challenge ou la solution CAPTCHA ne sont pas présents dans le jeton.
  - `rejected:expired`— L'horodatage du challenge ou du CAPTCHA du jeton a expiré, conformément aux durées d'immunité des jetons configurées par votre ACL Web.
  - `rejected:domain_mismatch`— Le domaine du jeton ne correspond pas à la configuration du domaine du jeton de votre ACL Web.
  - `rejected:invalid`— AWS WAF n'a pas pu lire le jeton indiqué.

  Exemple : les `awswaf:managed:captcha:rejected` libellés `awswaf:managed:captcha:rejected:expired` indiquent que la demande a été rejetée parce que l'horodatage CAPTCHA contenu dans le jeton a dépassé le délai d'immunité du jeton CAPTCHA configuré dans l'ACL Web.

- `absent`— La demande ne contient pas le jeton ou le gestionnaire de jetons n'a pas pu le lire.

  Exemple : L'étiquette `awswaf:managed:captcha:absent` indique que la demande ne contient pas le jeton.

Étiquettes ACFP

Ce groupe de règles génère des étiquettes avec le préfixe d'espace de noms `awswaf:managed:aws:acfp:` suivi de l'espace de noms personnalisé et du nom de l'étiquette. Le groupe de règles peut ajouter plusieurs libellés à une demande.

Vous pouvez récupérer toutes les étiquettes d'un groupe de règles via l'API en appelant`DescribeManagedRuleGroup`. Les étiquettes sont répertoriées dans la `AvailableLabels` propriété de la réponse.

Liste des règles de prévention des fraudes relatives à la création de comptes

Cette section répertorie les règles ACFP `AWSManagedRulesACFPRuleSet` et les étiquettes que les règles du groupe de règles ajoutent aux requêtes Web.

> **Note**
>
> Les informations que nous publions concernant les règles des groupes de règles AWS gérées sont destinées à vous fournir suffisamment d'informations pour utiliser les règles, sans fournir d'informations que des acteurs malveillants pourraient utiliser pour contourner les règles. Si vous avez besoin de plus d'informations que celles que vous trouverez dans cette documentation, contactez le AWS Support Centre.

Toutes les règles de ce groupe de règles nécessitent un jeton de requête Web, à l'exception des deux premières `UnsupportedCognitoIDP` et`AllRequests`. Pour une description des informations fournies par le jeton, consultezAWS WAF caractéristiques du jeton.

Sauf indication contraire, les règles de ce groupe de règles inspectent toutes les demandes que vos clients envoient aux chemins de page d'enregistrement et de création de compte que vous fournissez dans la configuration du groupe de règles. Pour plus d'informations sur la configuration de ce groupe de règles, consultezAWS WAF Contrôle des fraudes : création de comptes, prévention des fraudes (ACFP).

Nom de la règle	Description et étiquette
`UnsupportedCognitoIDP`	Vérifie le trafic Web destiné à un groupe d'utilisateurs Amazon Cognito. L'ACFP n'est pas disponible pour une utilisation avec les groupes d'utilisateurs Amazon Cognito, et cette règle permet de garantir que les autres règles du groupe de règles ACFP ne sont pas utilisées pour évaluer le trafic du groupe d'utilisateurs. Action de la règle Block Libellé : `awswaf:managed:aws:acfp:unsupported:cognito_idp`

Nom de la règle	Description et étiquette
`AllRequests`	Applique l'action de la règle aux demandes qui accèdent au chemin de la page d'enregis trement. Vous configurez le chemin de la page d'enregistrement lorsque vous configurez le groupe de règles. Par défaut, cette règle s'applique Challenge aux demandes. En appliquant cette action, la règle garantit que le client obtient un jeton de défi avant que les demandes ne soient évaluées par les autres règles du groupe de règles. Assurez-vous que vos utilisateurs finaux chargent le chemin de la page d'inscription avant de soumettre une demande de création de compte. Les jetons sont ajoutés aux demandes par les SDK d'intégration des applications clientes et par les actions de règles CAPTCHA etChallen ge. Pour l'acquisition de jetons la plus efficace possible, nous vous recommandons vivement d'utiliser les SDK d'intégration des applications. Pour plus d'informations, consultez AWS WAF intégration d'applications clientes. Action de la règle Challenge Étiquette : Aucune

Nom de la règle	Description et étiquette
`RiskScoreHigh`	Inspecte les demandes de création de compte contenant des adresses IP ou d'autres facteurs considérés comme hautement suspects. Cette évaluation est généralement basée sur plusieurs facteurs contributifs, que vous pouvez voir dans les `risk_score` libellés que le groupe de règles ajoute à la demande. Action de la règle Block Libellé : `awswaf:managed:aws:acfp:risk_score:high` La règle peut également s'appliquer `medium` ou des étiquettes de score de `low` risque à la demande. Si AWS WAF l'évaluation du score de risque pour la requête Web échoue, la règle ajoute l'étiquette `awswaf:managed:aws:acfp:risk_score:evaluation_failed` En outre, la règle ajoute des étiquettes avec l'espace de noms `awswaf:managed:aws:acfp:risk_score:contributor:` qui incluent le statut de l'évaluation du score de risque et les résultats pour les contributeurs spécifiques au score de risque, tels que les évaluations de réputation IP et d'informations d'identification volées.

Nom de la règle	Description et étiquette
`SignalCredentialCompromised`	Recherche dans la base de données des informations d'identification volées les informations d'identification qui ont été soumises dans la demande de création de compte. Cette règle garantit que les nouveaux clients initialisent leurs comptes avec une posture de sécurité positive. **Note** Vous pouvez ajouter une réponse de blocage personnalisée, pour décrire le problème à votre utilisateur final et lui indiquer comment procéder. Pour plus d'informations, veuillez consulter Exemple ACFP : réponse personnalisée pour des informations d'identification compromises. Action de la règle Block Libellé : `awswaf:managed:aws:acfp:signal:credential_compromised` Le groupe de règles applique l'étiquette associée suivante, mais ne prend aucune mesure, car les demandes de création de compte ne comporteront pas toutes des informations d'identification : `awswaf:managed:aws:acfp:signal:missing_credential`

Nom de la règle	Description et étiquette
`SignalClientHumanInteractivityAbsentLow`	Inspecte le jeton de la demande de création de compte à la recherche de données indiquant une interactivité humaine anormale avec l'application. L'interactivité humaine est détectée par le biais d'interactions telles que les mouvements de la souris et les pressions sur les touches. Si la page comporte un formulaire HTML, l'interactivité humaine inclut les interactions avec le formulaire. **Note** Cette règle inspecte uniquement les demandes relatives au chemin de création du compte et n'est évaluée que si vous avez implémenté les SDK d'intégration des applications. Les implémentations du SDK capturent passivement l'interactivité humaine et stockent les informations dans le jeton de demande. Pour plus d'informations, consultez AWS WAF caractéristiques du jeton et AWS WAF intégration d'applications clientes. Action de la règle CAPTCHA Libellé : Aucun. La règle détermine une correspondance en fonction de différents facteurs, de sorte qu'aucune étiquette individuelle ne s'applique à tous les scénarios de correspondance possibles.

Nom de la règle	Description et étiquette
	Le groupe de règles peut appliquer une ou plusieurs des étiquettes suivantes aux demandes : `awswaf:managed:aws:acfp:signal:client:human_interactivity:low/medium/high` `awswaf:managed:aws:acfp:signal:client:human_interactivity:insufficient_data` `awswaf:managed:aws:acfp:signal:form_detected` .
`SignalAutomatedBrowser`	Inspecte la demande à la recherche d'indicateurs indiquant que le navigateur client pourrait être automatisé. Action de la règle Block Libellé : `awswaf:managed:aws:acfp:signal:automated_browser`
`SignalBrowserInconsistency`	Inspecte le jeton de la demande pour détecter toute incohérence dans les données d'interrogation du navigateur. Pour plus d’informations, consultez AWS WAF caractéristiques du jeton. Action de la règle CAPTCHA Libellé : `awswaf:managed:aws:acfp:signal:browser_inconsistency`

Nom de la règle	Description et étiquette
`VolumetricIpHigh`	Détecte les volumes élevés de demandes de création de compte envoyées à partir d'adresses IP individuelles. Un volume élevé correspond à plus de 20 demandes dans une fenêtre de 10 minutes. **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. En cas de volume élevé, quelques demandes peuvent dépasser la limite avant que l'action de la règle ne soit appliquée. Action de la règle CAPTCHA Libellé : `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:high` La règle applique les libellés suivants aux demandes présentant un volume moyen (plus de 15 demandes par fenêtre de 10 minutes) et un faible volume (plus de 10 demandes par fenêtre de 10 minutes), mais ne prend aucune mesure à leur égard : `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:medium` et `awswaf:managed:aws:acfp:aggregate:volumetric:ip:creation:low` .

Nom de la règle	Description et étiquette
`VolumetricSessionHigh`	Inspecte les volumes élevés de demandes de création de compte envoyées lors de sessions client individuelles. Un volume élevé correspon d à plus de 10 demandes dans une fenêtre de 30 minutes. **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Quelques demandes peuvent dépasser la limite avant que l'action de la règle ne soit appliquée. Action de la règle Block Libellé : `awswaf:managed:aws:acfp:agg regate:volumetric:session:c reation:high` Le groupe de règles applique les libellés suivants aux demandes présentant un volume moyen (plus de 5 demandes par fenêtre de 30 minutes) et un volume faible (plus d'une demande par fenêtre de 30 minutes), mais ne prend aucune mesure à leur égard : `awswaf:managed:aws:acfp:agg regate:volumetric:session:c reation:medium` et `awswaf:ma naged:aws:acfp:aggregate:vo lumetric:session:creation:low` .

Nom de la règle	Description et étiquette
`AttributeUsernameTraversalHigh`	Détecte le taux élevé de demandes de création de compte provenant d'une seule session client utilisant des noms d'utilisateur différents. Le seuil pour une évaluation élevée est de plus de 10 demandes en 30 minutes. **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Quelques demandes peuvent dépasser la limite avant que l'action de la règle ne soit appliquée. Action de la règle Block Libellé : `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:high` Le groupe de règles applique les libellés suivants aux demandes présentant un volume moyen (plus de 5 demandes par fenêtre de 30 minutes) et un faible volume (plus d'une demande par fenêtre de 30 minutes) de demandes de traversée de nom d'utilisateur, mais ne prend aucune mesure à leur sujet : `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:medium` et `awswaf:managed:aws:acfp:aggregate:attribute:username_traversal:creation:low` .

Nom de la règle	Description et étiquette
`VolumetricPhoneNumberHigh`	Détecte les volumes élevés de demandes de création de compte utilisant le même numéro de téléphone. Le seuil pour une évaluation élevée est de plus de 10 demandes en 30 minutes. **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Quelques demandes peuvent dépasser la limite avant que l'action de la règle ne soit appliquée. Action de la règle Block Libellé : `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:high` Le groupe de règles applique les libellés suivants aux demandes présentant un volume moyen (plus de 5 demandes par fenêtre de 30 minutes) et un volume faible (plus d'une demande par fenêtre de 30 minutes), mais ne prend aucune mesure à leur égard : `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:medium` et `awswaf:managed:aws:acfp:aggregate:volumetric:phone_number:low` .

Nom de la règle	Description et étiquette
`VolumetricAddressHigh`	Détecte les volumes élevés de demandes de création de compte utilisant la même adresse physique. Le seuil pour une évaluation élevée est supérieur à 100 demandes par fenêtre de 30 minutes. **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Quelques demandes peuvent dépasser la limite avant que l'action de la règle ne soit appliquée. Action de la règle Block Libellé : `awswaf:managed:aws:acfp:aggregate:volumetric:address:high`

Nom de la règle	Description et étiquette
`VolumetricAddressLow`	Inspecte les volumes faibles et moyens de demandes de création de compte utilisant la même adresse physique. Le seuil pour une évaluation moyenne est supérieur à 50 demandes par fenêtre de 30 minutes, et pour une évaluation faible, il est supérieur à 10 demandes par fenêtre de 30 minutes. La règle applique l'action aux volumes moyens ou faibles. **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Quelques demandes peuvent dépasser la limite avant que l'action de la règle ne soit appliquée. Action de la règle CAPTCHA Étiquette : `awswaf:managed:aws:acfp:aggregate:volumetric:address:low` ou `awswaf:managed:aws:acfp:aggregate:volumetric:address:medium`

Nom de la règle	Description et étiquette
`VolumetricIPSuccessfulResponse`	Détecte un grand nombre de demandes de création de compte réussies pour une seule adresse IP. Cette règle regroupe les réponses positives de la ressource protégée aux demandes de création de compte. Le seuil pour une évaluation élevée est supérieur à 10 demandes par fenêtre de 10 minutes. Cette règle permet de se protéger contre les tentatives de création de comptes en masse. Son seuil est inférieur à celui de la règle`VolumetricIpHigh` , qui ne compte que les demandes. Si vous avez configuré le groupe de règles pour inspecter le corps de la réponse ou les composants JSON, vous AWS WAF pouvez inspecter les 65 536 premiers octets (64 Ko) de ces types de composants pour détecter des indicateurs de réussite ou d'échec. Cette règle applique l'action et l'étiquetage des règles aux nouvelles requêtes Web provenant d'une adresse IP, en fonction des réponses de réussite et d'échec de la ressource protégée aux récentes tentatives de connexion à partir de la même adresse IP. Vous définissez comment comptabiliser les réussites et les échecs lorsque vous configurez le groupe de règles. **Note** AWS WAF évalue cette règle uniquement dans les ACL Web qui

Nom de la règle	Description et étiquette
	protègent les distributions Amazon CloudFront . **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Il est possible que le client envoie plus de tentatives de création de compte réussies que celles autorisée s avant que la règle ne commence à correspondre lors des tentatives suivantes. Action de la règle Block Libellé : `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:high` Le groupe de règles applique également les libellés associés suivants aux demandes, sans aucune action associée. Tous les chiffres sont basés sur une fenêtre de 10 minutes. `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:medium` pour plus de 5 demandes réussies, `awswaf:managed:aws:acfp:aggregate:volumetric:ip:successful_creation_response:low` pour plus d'une demande réussie, `awswaf:ma`

Nom de la règle	Description et étiquette
	`naged:aws:acfp:aggregate:volumetric:ip:failed_creation_response:high` pour plus de 10 demandes ayant échoué, `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:medium` pour plus de 5 demandes ayant échoué et `awswaf:managed:aws:acfp:aggregate:volumetric:ip:failed_creation_response:low` pour plus d'une demande ayant échoué.

Nom de la règle	Description et étiquette
`VolumetricSessionSuccessful Response`	Vérifie s'il y a peu de réponses satisfaisantes de la ressource protégée aux demandes de création de compte envoyées à partir d'une seule session client. Cela permet de se protéger contre les tentatives de création de comptes en masse. Le seuil pour une évaluatio n faible est supérieur à 1 demande par fenêtre de 30 minutes. Cela permet de se protéger contre les tentative s de création de comptes en masse. Cette règle utilise un seuil inférieur à celui de la règle`VolumetricSessionHigh` , qui suit uniquement les demandes. Si vous avez configuré le groupe de règles pour inspecter le corps de la réponse ou les composants JSON, vous AWS WAF pouvez inspecter les 65 536 premiers octets (64 Ko) de ces types de composants pour détecter des indicateurs de réussite ou d'échec. Cette règle applique l'action et l'étiquetage des règles aux nouvelles requêtes Web provenant d'une session client, en fonction des réponses de réussite et d'échec de la ressource protégée aux récentes tentatives de connexion effectuée s au cours de la même session client. Vous définissez comment comptabiliser les réussites et les échecs lorsque vous configurez le groupe de règles.

Nom de la règle	Description et étiquette
	Note AWS WAF évalue cette règle uniquement dans les ACL Web qui protègent les distributions Amazon CloudFront .
	Note Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Il est possible que le client envoie plus de tentatives de création de compte infructueuses que ce qui est autorisé avant que la règle ne commence à correspondre lors des tentatives suivantes.
	Action de la règle Block Libellé : `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:low` Le groupe de règles applique également les libellés associés suivants aux demandes. Tous les comptes sont basés sur une fenêtre de 30 minutes. `awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_response:high` pour plus de 10 demandes réussies, `awswaf:managed:aws`

Nom de la règle	Description et étiquette
	`:acfp:aggregate:volumetric:session:successful_creation_response:medium` pour plus de 5 demandes réussies, `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:high` pour plus de 10 demandes ayant échoué, `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:medium` pour plus de 5 demandes ayant échoué et `awswaf:managed:aws:acfp:aggregate:volumetric:session:failed_creation_response:low` pour plus d'une demande ayant échoué.
`VolumetricSessionTokenReuseIp`	Inspecte les demandes de création de compte pour l'utilisation d'un seul jeton parmi plus de 5 adresses IP distinctes. **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Quelques demandes peuvent dépasser la limite avant que l'action de la règle ne soit appliquée. Action de la règle Block Libellé : `awswaf:managed:aws:acfp:aggregate:volumetric:session:creation:token_reuse:ip`

AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP)

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

L'ATP (AWS WAF Fraud Control Account Takeover Prevention) gère les étiquettes des groupes de règles et gère les demandes susceptibles de faire partie de tentatives malveillantes de prise de contrôle de compte. Pour ce faire, le groupe de règles inspecte les tentatives de connexion que les clients envoient au point de terminaison de connexion de votre application.

- Inspection des demandes — ATP vous donne de la visibilité et un contrôle sur les tentatives de connexion anormales et les tentatives de connexion utilisant des informations d'identification volées, afin d'empêcher les prises de contrôle de comptes susceptibles de mener à des activités frauduleuses. ATP vérifie les combinaisons d'e-mails et de mots de passe par rapport à sa base de données d'identifiants volés, qui est régulièrement mise à jour à mesure que de nouvelles informations d'identification divulguées sont découvertes sur le Dark Web. ATP agrège les données par adresse IP et par session client afin de détecter et de bloquer les clients qui envoient trop de demandes suspectes.
- Inspection des réponses — Pour les CloudFront distributions, en plus d'inspecter les demandes de connexion entrantes, le groupe de règles ATP inspecte les réponses de votre application aux tentatives de connexion, afin de suivre les taux de réussite et d'échec. À l'aide de ces informations, ATP peut bloquer temporairement les sessions client ou les adresses IP présentant trop d'échecs de connexion. AWS WAF effectue une inspection des réponses de manière asynchrone, afin de ne pas augmenter la latence de votre trafic Web.

Considérations relatives à l'utilisation de ce groupe de règles

Ce groupe de règles nécessite une configuration spécifique. Pour configurer et implémenter ce groupe de règles, consultez les instructions à l'adresseAWS WAF Contrôle des fraudes et prévention des prises de contrôle des comptes (ATP).

Ce groupe de règles fait partie des protections intelligentes d'atténuation des menaces contenues dans AWS WAF. Pour plus d’informations, veuillez consulter AWS WAF Atténuation intelligente des menaces.

> **Note**
>
> Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d’informations, consultez Tarification d’AWS WAF.

Pour réduire vos coûts et être sûr de gérer votre trafic Web comme vous le souhaitez, utilisez ce groupe de règles conformément aux instructions deMeilleures pratiques pour une atténuation intelligente des menaces.

Ce groupe de règles n'est pas disponible pour les groupes d'utilisateurs Amazon Cognito. Vous ne pouvez pas associer une ACL Web qui utilise ce groupe de règles à un groupe d'utilisateurs, ni ajouter ce groupe de règles à une ACL Web déjà associée à un groupe d'utilisateurs.

Étiquettes ajoutées par ce groupe de règles

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques d'Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

Étiquettes à jetons

Ce groupe de règles utilise la gestion des AWS WAF jetons pour inspecter et étiqueter les requêtes Web en fonction de l'état de leurs AWS WAF jetons. AWS WAF utilise des jetons pour le suivi et la vérification des sessions client.

Pour plus d'informations sur les jetons et la gestion des jetons, consultezAWS WAF jetons de demande Web.

Pour plus d'informations sur les composants de l'étiquette décrits ici, voirAWS WAF syntaxe des étiquettes et exigences de dénomination.

Libellé de session client

L'étiquette `awswaf:managed:token:id:`*`identifier`* contient un identifiant unique que la gestion des AWS WAF jetons utilise pour identifier la session client. L'identifiant peut changer si le client acquiert un nouveau jeton, par exemple après avoir supprimé le jeton qu'il utilisait.

> **Note**
>
> AWS WAF ne communique pas CloudWatch les statistiques Amazon pour cette étiquette.

Étiquettes d'état des jetons : préfixes d'espace de noms d'étiquettes

Les étiquettes d'état du jeton indiquent le statut du jeton et les informations de défi et de CAPTCHA qu'il contient.

Chaque étiquette de statut de jeton commence par l'un des préfixes d'espace de noms suivants :

- `awswaf:managed:token:` — Utilisé pour signaler l'état général du jeton et pour rendre compte de l'état des informations de défi du jeton.
- `awswaf:managed:captcha:` — Utilisé pour rendre compte de l'état des informations CAPTCHA du jeton.

Étiquettes d'état des jetons : noms des étiquettes

Après le préfixe, le reste de l'étiquette fournit des informations détaillées sur l'état du jeton :

- `accepted` — Le jeton de demande est présent et contient les éléments suivants :
  - Un défi ou une solution CAPTCHA valide.
  - Un défi ou un horodatage CAPTCHA non expiré.
  - Spécification de domaine valide pour l'ACL Web.

  Exemple : L'étiquette `awswaf:managed:token:accepted` indique que le jeton des requêtes Web contient une solution de défi valide, un horodatage de défi non expiré et un domaine valide.
- `rejected` — Le jeton de demande est présent mais ne répond pas aux critères d'acceptation.

  Outre l'étiquette rejetée, la gestion des jetons ajoute un espace de noms et un nom d'étiquette personnalisés pour en indiquer la raison.
  - `rejected:not_solved` — Le challenge ou la solution CAPTCHA ne sont pas présents dans le jeton.
  - `rejected:expired` — L'horodatage du challenge ou du CAPTCHA du jeton a expiré, conformément aux durées d'immunité des jetons configurées par votre ACL Web.
  - `rejected:domain_mismatch` — Le domaine du jeton ne correspond pas à la configuration du domaine du jeton de votre ACL Web.
  - `rejected:invalid` — AWS WAF n'a pas pu lire le jeton indiqué.

  Exemple : les `awswaf:managed:captcha:rejected` libellés `awswaf:managed:captcha:rejected:expired` indiquent que la demande a été rejetée parce que l'horodatage CAPTCHA contenu dans le jeton a dépassé le délai d'immunité du jeton CAPTCHA configuré dans l'ACL Web.

- `absent`— La demande ne contient pas le jeton ou le gestionnaire de jetons n'a pas pu le lire.

  Exemple : L'étiquette `awswaf:managed:captcha:absent` indique que la demande ne contient pas le jeton.

Étiquettes ATP

Le groupe de règles géré par ATP génère des étiquettes avec le préfixe d'espace de noms `awswaf:managed:aws:atp:` suivi de l'espace de noms personnalisé et du nom de l'étiquette.

Le groupe de règles peut ajouter l'une des étiquettes suivantes en plus des étiquettes indiquées dans la liste des règles :

- `awswaf:managed:aws:atp:signal:credential_compromised`— Indique que les informations d'identification soumises dans la demande se trouvent dans la base de données des informations d'identification volées.
- `awswaf:managed:aws:atp:aggregate:attribute:suspicious_tls_fingerprint`— Disponible uniquement pour les CloudFront distributions Amazon protégées. Indique qu'une session client a envoyé plusieurs demandes utilisant une empreinte TLS suspecte.
- `awswaf:managed:aws:atp:aggregate:volumetric:session:token_reuse:ip`— Indique l'utilisation d'un seul jeton parmi plus de 5 adresses IP distinctes. Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Quelques demandes peuvent dépasser la limite avant que l'étiquette ne soit appliquée.

Vous pouvez récupérer toutes les étiquettes d'un groupe de règles via l'API en appelant`DescribeManagedRuleGroup`. Les étiquettes sont répertoriées dans la `AvailableLabels` propriété de la réponse.

Liste des règles de prévention du piratage de compte

Cette section répertorie les règles ATP `AWSManagedRulesATPRuleSet` et les étiquettes que les règles du groupe de règles ajoutent aux requêtes Web.

> **Note**
>
> Les informations que nous publions concernant les règles des groupes de règles AWS gérées sont destinées à vous fournir suffisamment d'informations pour utiliser les règles, sans fournir d'informations que des acteurs malveillants pourraient utiliser pour contourner les

règles. Si vous avez besoin de plus d'informations que celles que vous trouverez dans cette documentation, contactez le AWS Support Centre.

Nom de la règle	Description et étiquette
`UnsupportedCognitoIDP`	Vérifie le trafic Web destiné à un groupe d'utilisateurs Amazon Cognito. ATP n'est pas disponible pour une utilisation avec les groupes d'utilisateurs Amazon Cognito, et cette règle permet de garantir que les autres règles des groupes de règles ATP ne sont pas utilisées pour évaluer le trafic des groupes d'utilisateurs. Action de la règle Block Libellé : `awswaf:managed:aws:atp:unsupported:cognito_idp`
`VolumetricIpHigh`	Détecte les volumes élevés de demandes envoyées à partir d'adresses IP individuelles. Un volume élevé correspond à plus de 20 demandes dans une fenêtre de 10 minutes. **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. En cas de volume élevé, quelques demandes peuvent dépasser la limite avant que l'action de la règle ne soit appliquée. Action de la règle Block

Nom de la règle	Description et étiquette
	Libellé : `awswaf:managed:aws:atp:aggregate:volumetric:ip:high` Le groupe de règles applique les libellés suivants aux demandes présentant un volume moyen (plus de 15 demandes par fenêtre de 10 minutes) et un volume faible (plus de 10 demandes par fenêtre de 10 minutes), mais ne prend aucune mesure à leur égard : `awswaf:managed:aws:atp:aggregate:volumetric:ip:medium` et`awswaf:managed:aws:atp:aggregate:volumetric:ip:low` .

Nom de la règle	Description et étiquette
`VolumetricSession`	Inspecte les volumes élevés de demandes envoyées lors de sessions client individue lles. Le seuil est supérieur à 20 demandes par fenêtre de 30 minutes. Cette inspection ne s'applique que lorsque la requête Web contient un jeton. Les jetons sont ajoutés aux demandes par les SDK d'intégra tion des applications et par les actions de règles CAPTCHA etChallenge. Pour plus d'informations, consultez AWS WAF jetons de demande Web. **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Quelques demandes peuvent dépasser la limite avant que l'action de la règle ne soit appliquée. Action de la règle Block Libellé : `awswaf:managed:aws:atp:aggr egate:volumetric:session`

Nom de la règle	Description et étiquette
`AttributeCompromisedCredentials`	Vérifie la présence de plusieurs demandes provenant de la même session client qui utilisent des informations d'identification volées. Action de la règle Block Libellé : `awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials`
`AttributeUsernameTraversal`	Vérifie la présence de plusieurs demandes provenant de la même session client qui utilisent le changement de nom d'utilisateur. Action de la règle Block Libellé : `awswaf:managed:aws:atp:aggregate:attribute:username_traversal`
`AttributePasswordTraversal`	Vérifie la présence de plusieurs demandes utilisant le même nom d'utilisateur et utilisant la traversée de mots de passe. Action de la règle Block Libellé : `awswaf:managed:aws:atp:aggregate:attribute:password_traversal`

Nom de la règle	Description et étiquette
`AttributeLongSession`	Vérifie la présence de plusieurs demandes provenant de la même session client qui utilisent des sessions de longue durée. Le seuil est de plus de 6 heures de trafic faisant l'objet d'au moins une demande de connexion toutes les 30 minutes. Cette inspection ne s'applique que lorsque la requête Web contient un jeton. Les jetons sont ajoutés aux demandes par les SDK d'intégration des applications et par les actions de règles CAPTCHA etChallenge. Pour plus d'informations, consultez AWS WAF jetons de demande Web. Action de la règle Block Libellé : `awswaf:managed:aws:atp:aggregate:attribute:long_session`

Nom de la règle	Description et étiquette
`TokenRejected`	Inspecte les demandes contenant des jetons qui sont rejetées par la gestion des AWS WAF jetons. Cette inspection ne s'applique que lorsque la requête Web contient un jeton. Les jetons sont ajoutés aux demandes par les SDK d'intégration des applications et par les actions de règles CAPTCHA etChallenge. Pour plus d'informations, consultez AWS WAF jetons de demande Web. Action de la règle Block Libellé : Aucun Pour vérifier si un jeton a été rejeté, utilisez une règle de correspondance d'étiquette correspondant à l'étiquette : `awswaf:managed:token:rejected`
`SignalMissingCredential`	Vérifie les demandes dont les informations d'identification ne contiennent pas le nom d'utilisateur ou le mot de passe. Action de la règle Block Libellé : `awswaf:managed:aws:atp:signal:missing_credential`

Nom de la règle	Description et étiquette
`VolumetricIpFailedLoginResponseHigh`	Recherche les adresses IP qui ont récemment été à l'origine d'un taux trop élevé de tentatives de connexion infructueuses. Un volume élevé correspond à plus de 10 demandes de connexion échouées provenant d'une adresse IP dans une fenêtre de 10 minutes. Si vous avez configuré le groupe de règles pour inspecter le corps de la réponse ou les composants JSON, vous AWS WAF pouvez inspecter les 65 536 premiers octets (64 Ko) de ces types de composants pour détecter des indicateurs de réussite ou d'échec. Cette règle applique l'action et l'étiquetage des règles aux nouvelles requêtes Web provenant d'une adresse IP, en fonction des réponses de réussite et d'échec de la ressource protégée aux récentes tentatives de connexion à partir de la même adresse IP. Vous définissez comment comptabiliser les réussites et les échecs lorsque vous configurez le groupe de règles. **Note** AWS WAF évalue cette règle uniquement dans les ACL Web qui protègent les distributions Amazon CloudFront.

Nom de la règle	Description et étiquette
	Note Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Il est possible que le client envoie plus de tentatives de connexion infructueuses que ce qui est autorisé avant que la règle ne commence à correspondre lors des tentatives suivantes. Action de la règle Block Libellé : `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` Le groupe de règles applique également les libellés associés suivants aux demandes, sans aucune action associée. Tous les chiffres sont basés sur une fenêtre de 10 minutes. `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:medium` pour plus de 5 demandes ayant échoué, `awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:low` pour plus d'une demande échouée, `awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:high` pour plus de 10 demandes réussies, `awswaf:managed:aws:atp:aggregate:volumetric:ip:success`

Nom de la règle	Description et étiquette
	`ful_login_response:medium` pour plus de 5 demandes réussies et `awswaf:managed:aws:atp:aggregate:volumetric:ip:successful_login_response:low` pour plus d'une demande réussie.

Nom de la règle	Description et étiquette
`VolumetricSessionFailedLogi nResponseHigh`	Vérifie les sessions client qui ont récemment été à l'origine d'un taux trop élevé de tentative s de connexion infructueuses. Un volume élevé correspond à plus de 10 demandes de connexion échouées depuis une session client sur une période de 30 minutes. Si vous avez configuré le groupe de règles pour inspecter le corps de la réponse ou les composants JSON, vous AWS WAF pouvez inspecter les 65 536 premiers octets (64 Ko) de ces types de composants pour détecter des indicateurs de réussite ou d'échec. Cette règle applique l'action et l'étiquetage des règles aux nouvelles requêtes Web provenant d'une session client, en fonction des réponses de réussite et d'échec de la ressource protégée aux récentes tentatives de connexion effectuée s au cours de la même session client. Vous définissez comment comptabiliser les réussites et les échecs lorsque vous configurez le groupe de règles. **Note** AWS WAF évalue cette règle uniquement dans les ACL Web qui protègent les distributions Amazon CloudFront .

Nom de la règle	Description et étiquette
	Note Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Il est possible que le client envoie plus de tentatives de connexion infructueuses que ce qui est autorisé avant que la règle ne commence à correspondre lors des tentatives suivantes. Cette inspection ne s'applique que lorsque la requête Web contient un jeton. Les jetons sont ajoutés aux demandes par les SDK d'intégration des applications et par les actions de règles CAPTCHA etChallenge. Pour plus d'informations, consultez AWS WAF jetons de demande Web. Action de la règle Block Libellé : `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:high` Le groupe de règles applique également les libellés associés suivants aux demandes, sans aucune action associée. Tous les comptes sont basés sur une fenêtre de 30 minutes. `awswaf:managed:aws:atp:aggregate:volumetric:session:failed_login_response:medium` pour plus de 5 demandes ayant échoué, `awswaf:managed:aws`

Nom de la règle	Description et étiquette
	`:atp:aggregate:volumetric:session:failed_login_response:low` pour plus d'une demande échouée, `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:high` pour plus de 10 demandes réussies, `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:medium` pour plus de 5 demandes réussies et `awswaf:managed:aws:atp:aggregate:volumetric:session:successful_login_response:low` pour plus d'une demande réussie.

AWS WAF Groupe de règles Bot Control

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

Le groupe de règles gérées par Bot Control fournit des règles qui gèrent les demandes des robots. Les robots peuvent consommer des ressources excédentaires, fausser les indicateurs commerciaux, provoquer des interruptions de service et mener des activités malveillantes.

Niveaux de protection

Le groupe de règles gérées par Bot Control fournit deux niveaux de protection parmi lesquels vous pouvez choisir :

- Fréquent : détecte une variété de robots auto-identifiables, tels que les frameworks de scraping Web, les moteurs de recherche et les navigateurs automatisés. Les protections Bot Control à ce niveau identifient les robots courants à l'aide de techniques de détection de bots traditionnelles, telles que l'analyse statique des données des demandes. Les règles étiquettent le trafic provenant de ces robots et bloquent ceux qu'ils ne peuvent pas vérifier.
- Ciblé : inclut les protections de niveau commun et ajoute une détection ciblée pour les robots sophistiqués qui ne s'identifient pas eux-mêmes. Des protections ciblées atténuent l'activité des

robots en combinant la limitation du débit, le CAPTCHA et les défis liés au navigateur en arrière-plan.

- **`TGT_`**— Les règles qui fournissent une protection ciblée portent des noms commençant par`TGT_`. Toutes les protections ciblées utilisent des techniques de détection telles que l'interrogation du navigateur, la prise d'empreintes digitales et l'heuristique comportementale pour identifier le trafic de bots défectueux.
- **`TGT_ML_`**— Les règles de protection ciblées qui utilisent l'apprentissage automatique portent des noms commençant par`TGT_ML_`. Ces règles utilisent une analyse automatisée par apprentissage automatique des statistiques de trafic du site Web pour détecter les comportements anormaux indiquant une activité distribuée et coordonnée des bots. AWS WAF analyse les statistiques relatives au trafic de votre site Web, telles que les horodatages, les caractéristiques du navigateur et les URL précédemment visitées, afin d'améliorer le modèle d'apprentissage automatique de Bot Control. Les fonctionnalités d'apprentissage automatique sont activées par défaut, mais vous pouvez les désactiver dans la configuration de votre groupe de règles. Lorsque l'apprentissage automatique est désactivé, AWS WAF n'évalue pas ces règles.

Le niveau de protection ciblé et l'énoncé de règle AWS WAF basé sur le taux permettent tous deux de limiter le débit. Pour une comparaison des deux options, voirOptions de limitation du débit dans les règles basées sur les taux et dans les règles de contrôle des bots ciblées.

Considérations relatives à l'utilisation de ce groupe de règles

Ce groupe de règles fait partie des protections intelligentes d'atténuation des menaces contenues dans AWS WAF. Pour plus d’informations, veuillez consulter AWS WAF Atténuation intelligente des menaces.

> **Note**
>
> Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d’informations, consultez Tarification d’AWS WAF.

Pour réduire vos coûts et être sûr de gérer votre trafic Web comme vous le souhaitez, utilisez ce groupe de règles conformément aux instructions deMeilleures pratiques pour une atténuation intelligente des menaces.

Nous mettons régulièrement à jour nos modèles d'apprentissage automatique (ML) pour les règles basées sur le niveau de protection ciblé, afin d'améliorer les prévisions des robots. Les règles basées sur le ML ont des noms commençant par. `TGT_ML_` Si vous remarquez un changement soudain et substantiel dans les prédictions des robots établies par ces règles, contactez-nous par l'intermédiaire de votre responsable de compte ou ouvrez un dossier auprès AWS Support du Center.

Étiquettes ajoutées par ce groupe de règles

Ce groupe de règles géré ajoute des libellés aux requêtes Web qu'il évalue, qui sont disponibles pour les règles exécutées après ce groupe de règles dans votre ACL Web. AWS WAF enregistre également les étiquettes selon les CloudWatch statistiques d'Amazon. Pour obtenir des informations générales sur les étiquettes et les mesures relatives aux étiquettes, reportez-vous Étiquettes sur les requêtes Web aux sections etMétriques et dimensions des étiquettes.

Étiquettes à jetons

Ce groupe de règles utilise la gestion des AWS WAF jetons pour inspecter et étiqueter les requêtes Web en fonction de l'état de leurs AWS WAF jetons. AWS WAF utilise des jetons pour le suivi et la vérification des sessions client.

Pour plus d'informations sur les jetons et leur gestion, consultezAWS WAF jetons de demande Web.

Pour plus d'informations sur les composants de l'étiquette décrits ici, voirAWS WAF syntaxe des étiquettes et exigences de dénomination.

Libellé de session client

L'étiquette `awswaf:managed:token:id:`*`identifier`* contient un identifiant unique que la gestion des AWS WAF jetons utilise pour identifier la session client. L'identifiant peut changer si le client acquiert un nouveau jeton, par exemple après avoir supprimé le jeton qu'il utilisait.

> **Note**
>
> AWS WAF ne communique pas CloudWatch les statistiques Amazon pour cette étiquette.

Étiquettes d'état des jetons : préfixes d'espace de noms d'étiquettes

Les étiquettes d'état du jeton indiquent le statut du jeton ainsi que les informations relatives au défi et au CAPTCHA qu'il contient.

Chaque étiquette de statut de jeton commence par l'un des préfixes d'espace de noms suivants :

- `awswaf:managed:token:` — Utilisé pour signaler l'état général du jeton et pour rendre compte de l'état des informations de défi du jeton.
- `awswaf:managed:captcha:` — Utilisé pour rendre compte de l'état des informations CAPTCHA du jeton.

Étiquettes d'état des jetons : noms des étiquettes

Après le préfixe, le reste de l'étiquette fournit des informations détaillées sur l'état du jeton :

- `accepted` — Le jeton de demande est présent et contient les éléments suivants :
  - Un défi ou une solution CAPTCHA valide.
  - Un défi ou un horodatage CAPTCHA non expiré.
  - Spécification de domaine valide pour l'ACL Web.

  Exemple : L'étiquette `awswaf:managed:token:accepted` indique que le jeton des requêtes Web contient une solution de défi valide, un horodatage de défi non expiré et un domaine valide.
- `rejected` — Le jeton de demande est présent mais ne répond pas aux critères d'acceptation.

  Outre l'étiquette rejetée, la gestion des jetons ajoute un espace de noms et un nom d'étiquette personnalisés pour en indiquer la raison.
  - `rejected:not_solved` — Le challenge ou la solution CAPTCHA ne sont pas présents dans le jeton.
  - `rejected:expired` — L'horodatage du challenge ou du CAPTCHA du jeton a expiré, conformément aux durées d'immunité des jetons configurées par votre ACL Web.
  - `rejected:domain_mismatch` — Le domaine du jeton ne correspond pas à la configuration du domaine du jeton de votre ACL Web.
  - `rejected:invalid` — AWS WAF n'a pas pu lire le jeton indiqué.

  Exemple : les `awswaf:managed:captcha:rejected` libellés `awswaf:managed:captcha:rejected:expired` indiquent que la demande a été rejetée parce que l'horodatage CAPTCHA contenu dans le jeton a dépassé le délai d'immunité du jeton CAPTCHA configuré dans l'ACL Web.
- `absent` — La demande ne contient pas le jeton ou le gestionnaire de jetons n'a pas pu le lire.

  Exemple : L'étiquette `awswaf:managed:captcha:absent` indique que la demande ne contient pas le jeton.

Étiquettes Bot Control

Le groupe de règles géré par Bot Control génère des étiquettes avec le préfixe d'espace de noms `awswaf:managed:aws:bot-control:` suivi de l'espace de noms personnalisé et du nom de l'étiquette. Le groupe de règles peut ajouter plusieurs libellés à une demande.

Chaque étiquette reflète les conclusions de la règle Bot Control :

- `awswaf:managed:aws:bot-control:bot:`— Informations sur le bot associé à la demande.
  - `awswaf:managed:aws:bot-control:bot:name:<name>`— Le nom du bot, s'il est disponible, par exemple, les espaces de noms personnalisés `bot:name:slurp`et `bot:name:googlebot`, et`bot:name:pocket_parser`.
  - `awswaf:managed:aws:bot-control:bot:category:<category>`— La catégorie du bot, telle que définie par AWS WAF, par exemple, `bot:category:search_engine` et`bot:category:content_fetcher`.
  - `awswaf:managed:aws:bot-control:bot:organization:<organization>`— L'éditeur du bot, par exemple,`bot:organization:google`.
  - `awswaf:managed:aws:bot-control:bot:verified`— Utilisé pour indiquer un bot qui s'identifie et que Bot Control a pu vérifier. Ceci est utilisé pour les robots les plus courants et peut être utile lorsqu'il est combiné avec des étiquettes de catégorie `bot:category:search_engine` ou des étiquettes de nom telles que`bot:name:googlebot`.

    > **Note**
    >
    > Bot Control utilise l'adresse IP de l'origine de la requête Web pour déterminer si un bot est vérifié. Vous ne pouvez pas le configurer pour utiliser la configuration IP AWS WAF transférée, pour inspecter une autre source d'adresses IP. Si vous avez vérifié que des robots sont acheminés via un proxy ou un équilibreur de charge, vous pouvez ajouter une règle qui s'exécute avant le groupe de règles Bot Control pour vous aider. Configurez votre nouvelle règle pour utiliser l'adresse IP transférée et autoriser explicitement les demandes provenant des robots vérifiés. Pour plus d'informations sur l'utilisation des adresses IP transférées, consultezAdresse IP transférée.

  - `awswaf:managed:aws:bot-control:bot:user_triggered:verified`— Utilisé pour indiquer un bot similaire à un bot vérifié, mais qui peut être directement invoqué par les utilisateurs finaux. Cette catégorie de bot est traitée par les règles du Bot Control comme un bot non vérifié.

  - `awswaf:managed:aws:bot-control:bot:developer_platform:verified`— Utilisé pour indiquer un bot similaire à un bot vérifié, mais utilisé par les plateformes de développement pour la création de scripts, par exemple Google Apps Script. Cette catégorie de bot est traitée par les règles du Bot Control comme un bot non vérifié.
  - `awswaf:managed:aws:bot-control:bot:unverified`— Utilisé pour indiquer un bot qui s'identifie, afin qu'il puisse être nommé et classé, mais qui ne publie pas d'informations pouvant être utilisées pour vérifier son identité de manière indépendante. Ces types de signatures de robots peuvent être falsifiés et sont donc considérés comme non vérifiés.
- `awswaf:managed:aws:bot-control:targeted:<additional-details>` — Utilisé pour les étiquettes spécifiques aux protections ciblées Bot Control.
- `awswaf:managed:aws:bot-control:signal:<signal-details>`et `awswaf:managed:aws:bot-control:targeted:signal:<signal-details>` — Utilisé pour fournir des informations supplémentaires sur la demande dans certaines situations.

  Voici des exemples d'étiquettes de signal. Cette liste n'est pas exhaustive :

  - `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`— Indique la détection d'une extension de navigateur qui facilite l'automatisation, telle que Selenium IDE.

    Cette étiquette est ajoutée chaque fois qu'un utilisateur a installé ce type d'extension, même s'il ne l'utilise pas activement. Si vous implémentez une règle de correspondance des libellés à cet effet, soyez conscient de la possibilité de faux positifs dans la logique de la règle et dans les paramètres d'action. Par exemple, vous pouvez utiliser une CAPTCHA action à la place de Block ou vous pouvez combiner cette correspondance d'étiquette avec d'autres correspondances d'étiquettes, afin de vous assurer que l'automatisation est utilisée.
  - `awswaf:managed:aws:bot-control:signal:automated_browser`— Indique que la demande contient des indicateurs indiquant que le navigateur client est peut-être automatisé.
  - `awswaf:managed:aws:bot-control:targeted:signal:automated_browser`— Indique que le AWS WAF jeton de la demande contient des indicateurs indiquant que le navigateur client est peut-être automatisé.

Vous pouvez récupérer toutes les étiquettes d'un groupe de règles via l'API en appelant`DescribeManagedRuleGroup`. Les étiquettes sont répertoriées dans la `AvailableLabels` propriété de la réponse.

Le groupe de règles géré par Bot Control applique des étiquettes à un ensemble de robots vérifiables généralement autorisés. Le groupe de règles ne bloque pas ces robots vérifiés. Si vous le souhaitez, vous pouvez les bloquer, ou un sous-ensemble d'entre eux, en écrivant une règle personnalisée qui utilise les étiquettes appliquées par le groupe de règles géré par Bot Control. Pour plus d'informations à ce sujet et pour des exemples, consultezAWS WAF Contrôle des robots.

Liste des règles de contrôle des bots

Cette section répertorie les règles de contrôle des robots.

> **Note**
>
> Les informations que nous publions concernant les règles des groupes de règles AWS gérées sont destinées à vous fournir suffisamment d'informations pour utiliser les règles, sans fournir d'informations que des acteurs malveillants pourraient utiliser pour contourner les règles. Si vous avez besoin de plus d'informations que celles que vous trouverez dans cette documentation, contactez le AWS Support Centre.

Nom de la règle	Description
`CategoryAdvertising`	Inspecte les robots utilisés à des fins publicitaires. Par exemple, vous pouvez utiliser des services publicitaires tiers qui doivent accéder par programmation à votre site Web. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:advertising` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .
`CategoryArchiver`	

Nom de la règle	Description
	Inspecte les robots utilisés à des fins d'archiva ge. Ces robots explorent le Web et capturent du contenu dans le but de créer des archives. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-cont rol:bot:category:archiver` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws :bot-control:bot:verified` .
`CategoryContentFetcher`	Détecte les robots qui visitent le site Web de l'application pour le compte d'un utilisateur, pour récupérer du contenu tel que des flux RSS ou pour vérifier ou valider votre contenu. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot- control:bot:category:content_fe tcher` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws :bot-control:bot:verified` .

Nom de la règle	Description
`CategoryEmailClient`	Détecte les robots qui vérifient les liens contenus dans les e-mails pointant vers le site Web de l'application. Cela peut inclure des robots gérés par des entreprises et des fournisseurs de messagerie, pour vérifier les liens contenus dans les e-mails et signaler les e-mails suspects. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:email_client` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .
`CategoryHttpLibrary`	Inspecte les requêtes générées par des robots à partir des bibliothèques HTTP de différents langages de programmation. Il peut s'agir de demandes d'API que vous choisissez d'autoriser ou de surveiller. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:http_library` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .

Nom de la règle	Description
`CategoryLinkChecker`	Détecte les robots qui vérifient la présence de liens rompus. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:link_checker` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .
`CategoryMiscellaneous`	Inspecte les robots divers qui ne correspondent pas aux autres catégories. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:miscellaneous` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .

Nom de la règle	Description
`CategoryMonitoring`	Inspecte les robots utilisés à des fins de surveillance. Par exemple, vous pouvez utiliser des services de surveillance de bots qui envoient régulièrement des requêtes ping au site Web de votre application pour surveiller des éléments tels que les performances et le temps de disponibilité. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:monitoring` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .
`CategoryScrapingFramework`	Inspecte les robots à partir des frameworks de scraping Web, qui sont utilisés pour automatiser l'exploration et l'extraction du contenu des sites Web. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:scraping_framework` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .

Nom de la règle	Description
`CategorySearchEngine`	Inspecte les robots des moteurs de recherche , qui explorent les sites Web pour indexer le contenu et rendre les informations disponibles pour les résultats des moteurs de recherche. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:search_engine` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .
`CategorySecurity`	Détecte les robots qui analysent les applications Web à la recherche de vulnérabilités ou qui effectuent des audits de sécurité. Par exemple, vous pouvez faire appel à un fournisseur de sécurité tiers qui analyse, surveille ou audite la sécurité de votre application Web. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:security` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .

Nom de la règle	Description
`CategorySeo`	Inspecte les robots utilisés pour l'optimisation des moteurs de recherche. Par exemple, vous pouvez utiliser des outils de moteur de recherche qui explorent votre site pour vous aider à améliorer votre classement dans les moteurs de recherche. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:seo` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .
`CategorySocialMedia`	Détecte les robots utilisés par les plateformes de réseaux sociaux pour fournir des résumés de contenu lorsque les utilisateurs partagent votre contenu. Action de règle, appliquée uniquement aux robots non vérifiés : Block Libellé : `awswaf:managed:aws:bot-control:bot:category:social_media` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .

Nom de la règle	Description
`CategoryAI`	Inspecte les robots dotés d'intelligence artificielle (IA). Action de la règle Block Libellé : `awswaf:managed:aws:bot-control:bot:category:ai`
`SignalAutomatedBrowser`	Inspecte la demande à la recherche d'indicateurs indiquant que le navigateur client pourrait être automatisé. Les navigateurs automatisés peuvent être utilisés pour les tests ou le scraping. Par exemple, vous pouvez utiliser ces types de navigateurs pour surveiller ou vérifier le site Web de votre application. Action de la règle Block Libellé : `awswaf:managed:aws:bot-control:signal:automated_browser`
`SignalKnownBotDataCenter`	Inspecte les indicateurs des centres de données généralement utilisés par les robots. Action de la règle Block Libellé : `awswaf:managed:aws:bot-control:signal:known_bot_data_center`

Nom de la règle	Description
`SignalNonBrowserUserAgent`	Vérifie la présence de chaînes d'agent utilisateur qui ne semblent pas provenir d'un navigateur Web. Cette catégorie peut inclure les demandes d'API. Action de la règle Block Libellé : `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`

Nom de la règle	Description
`TGT_VolumetricIpTokenAbsent`	Vérifie la présence de 5 demandes ou plus émanant d'un client au cours des 5 dernières minutes qui n'incluent pas de jeton de défi valide. Pour plus d'informations sur les jetons, consultezAWS WAF jetons de demande Web. **Note** Il est possible que cette règle correspon de à une demande contenant un jeton si des jetons ont récemment été manquants dans les demandes du même client. Le seuil appliqué par cette règle peut varier légèrement en raison de la latence. Cette règle gère les jetons manquants différemment de l'étiquetage des jetons :`awswaf:managed:token:absent` . L'étiquetage des jetons permet d'étiquet er les demandes individuelles qui n'ont pas de jeton. Cette règle tient à jour le nombre de demandes dont le jeton est manquant pour chaque adresse IP du client, et elle le compare aux demandes dont le jeton dépasse la limite. Action de règle, appliquée uniquement aux clients qui ne sont pas des robots vérifiés : Challenge Libellé : `awswaf:managed:aws:bot-control:targeted:aggregate:volu metric:ip:token_absent`

Nom de la règle	Description
	Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws :bot-control:bot:verified` .

Nom de la règle	Description
`TGT_VolumetricSession`	Détecte un nombre anormalement élevé de demandes provenant d'une session client par fenêtre de 5 minutes. L'évaluation est basée sur une comparaison avec des lignes de base volumétriques standard qui utilisent les AWS WAF modèles de trafic historiques. Cette inspection ne s'applique que lorsque la requête Web contient un jeton. Les jetons sont ajoutés aux demandes par les SDK d'intégration des applications et par les actions de règles CAPTCHA etChallenge. Pour plus d'informations, consultez AWS WAF jetons de demande Web. **Note** L'entrée en vigueur de cette règle peut prendre 5 minutes après son activation. Bot Control identifie les comportements anormaux de votre trafic Web en comparant le trafic actuel aux bases de trafic calculées. AWS WAF Action de règle, appliquée uniquement aux clients qui ne sont pas des robots vérifiés : CAPTCHA Libellé : `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:high`

Nom de la règle	Description
	Le groupe de règles applique les libellés suivants aux demandes de volume moyen et inférieur supérieures à un seuil minimum. Pour ces niveaux, la règle ne prend aucune action, que le client soit vérifié ou non : `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:medium` et `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:low` . Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé `awswaf:managed:aws:bot-control:bot:verified` .

Nom de la règle	Description
`TGT_SignalAutomatedBrowser`	Inspecte le jeton de la demande à la recherche d'indicateurs indiquant que le navigateur client pourrait être automatisé. Pour plus d'informations, consultez AWS WAF caractéristiques du jeton. Cette inspection ne s'applique que lorsque la requête Web contient un jeton. Les jetons sont ajoutés aux demandes par les SDK d'intégration des applications et par les actions de règles CAPTCHA etChallenge. Pour plus d'informations, consultez AWS WAF jetons de demande Web. Action de règle, appliquée uniquement aux clients qui ne sont pas des robots vérifiés : CAPTCHA Libellé : `awswaf:managed:aws:bot-control:targeted:signal:automated_browser` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .

Nom de la règle	Description
`TGT_SignalBrowserInconsistency`	Inspecte les données d'interrogation du navigateur pour détecter toute incohérence. Pour plus d'informations, consultez AWS WAF caractéristiques du jeton. Cette inspection ne s'applique que lorsque la requête Web contient un jeton. Les jetons sont ajoutés aux demandes par les SDK d'intégration des applications et par les actions de règles CAPTCHA etChallenge. Pour plus d'informations, consultez AWS WAF jetons de demande Web. Action de règle, appliquée uniquement aux clients qui ne sont pas des robots vérifiés : CAPTCHA Libellé : `awswaf:managed:aws:bot-control:targeted:signal:browser_inconsistency` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` .

Nom de la règle	Description
`TGT_TokenReuseIp`	Vérifie l'utilisation d'un seul jeton parmi plus de 5 adresses IP distinctes. **Note** Les seuils appliqués par cette règle peuvent varier légèrement en raison de la latence. Quelques demandes peuvent dépasser la limite avant que l'action de la règle ne soit appliquée. Action de la règle Count Libellé : `awswaf:managed:aws:bot-control:targeted:aggregate:volumetric:session:token_reuse:ip`

Nom de la règle	Description
`TGT_ML_CoordinatedActivityMedium` et `TGT_ML_CoordinatedActivityHigh`	Détectez tout comportement anormal correspondant à une activité distribuée et coordonnée des bots. Les niveaux de règles indiquent le niveau de confiance selon lequel un groupe de demandes participe à une attaque coordonnée. **Note** Ces règles ne s'exécutent que si le groupe de règles est configuré pour utiliser l'apprentissage automatique (ML). Pour plus d'informations sur la configuration de ce choix, consultez Ajout du groupe de règles géré par AWS WAF Bot Control à votre ACL Web. AWS WAF effectue cette inspection par le biais d'une analyse par apprentissage automatique des statistiques de trafic du site Web. AWS WAF analyse le trafic Web toutes les quelques minutes et optimise l'analyse pour détecter les robots de faible intensité et de longue durée répartis sur de nombreuses adresses IP. Ces règles peuvent correspondre sur un très petit nombre de demandes avant de déterminer qu'une attaque coordonnée n'est pas en cours. Donc, si vous ne voyez qu'une ou deux correspondances, les résultats peuvent être des faux positifs. Cependant, si vous voyez de nombreux matchs échapper à ces règles,

Nom de la règle	Description
	vous êtes probablement victime d'une attaque coordonnée. **Note** Ces règles peuvent prendre jusqu'à 24 heures pour entrer en vigueur une fois que vous avez activé les règles ciblées Bot Control avec l'option ML. Bot Control identifie les comportem ents anormaux de votre trafic Web en comparant le trafic actuel aux bases de trafic calculées AWS WAF . AWS WAF calcule les lignes de base uniquement lorsque vous utilisez les règles ciblées Bot Control avec l'option ML, et l'établis sement de bases de référence significa tives peut prendre jusqu'à 24 heures. Nous mettons régulièrement à jour nos modèles d'apprentissage automatique en fonction de ces règles, afin d'améliorer les prévisions des robots. Si vous remarquez un changement soudain et substantiel dans les prédictions des robots établies par ces règles, contactez votre responsable de compte ou ouvrez un dossier auprès AWS Support du Center. Actions de règles, appliquées uniquement aux clients qui ne sont pas des robots vérifiés : • Moyenne : Count •

Nom de la règle	Description
	Élevée : Count Étiquettes : `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:medium` et `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:high` Pour les robots vérifiés, le groupe de règles n'effectue aucune action, mais il ajoute le libellé des règles et le libellé`awswaf:managed:aws:bot-control:bot:verified` . Le groupe de règles ajoute également l'étiquette `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low` pour indiquer un faible niveau de confiance, mais il n'applique aucune règle et ne prend aucune mesure pour ces demandes.

Déploiements pour les groupes de règles AWS gérées versionnés

AWS déploie les modifications apportées à ses groupes de règles AWS gérées versionnés dans trois déploiements standard : version candidate, version statique et version par défaut. En outre, il AWS peut parfois être nécessaire de publier un déploiement d'exception ou d'annuler le déploiement d'une version par défaut.

> **Note**
>
> Cette section s'applique uniquement aux groupes de règles AWS gérées qui sont versionnés. Le seul groupe de règles qui n'est pas versionné est le groupe de règles de réputation IP.

Rubriques

Notifications pour les déploiements de groupes de règles AWS gérées

Les groupes de règles AWS gérées versionnés fournissent tous des notifications de mise à jour SNS pour les déploiements et utilisent tous la même rubrique SNS Amazon Resource Name (ARN). Le seul groupe de règles qui n'est pas versionné est le groupe de règles de réputation IP.

Pour les déploiements qui affectent vos protections, tels que les modifications apportées à la version par défaut, AWS fournit des notifications SNS pour vous informer des déploiements planifiés et pour vous indiquer quand un déploiement commence. Pour les déploiements qui n'affectent pas vos protections, tels que les déploiements de versions candidates et de versions statiques, vous pouvez AWS être averti une fois le déploiement commencé ou même une fois celui-ci terminé. Une fois le déploiement d'une nouvelle version statique terminé, AWS met à jour ce guide, dans le journal des modifications AWS Journal des modifications des règles gérées et dans la page d'historique du document à l'adresse. Historique du document

Pour recevoir toutes les AWS mises à jour relatives aux groupes de règles AWS gérées, abonnez-vous au flux RSS depuis n'importe quelle page HTML de ce guide et abonnez-vous à la rubrique SNS relative aux groupes de règles AWS gérées. Pour plus d'informations sur l'abonnement aux notifications SNS, consultez. Être informé des nouvelles versions et des mises à jour d'un groupe de règles géré

Contenu des notifications SNS

Les champs des notifications Amazon SNS incluent toujours l'objet, le message et. MessageAttributes Les champs supplémentaires dépendent du type de message et du groupe

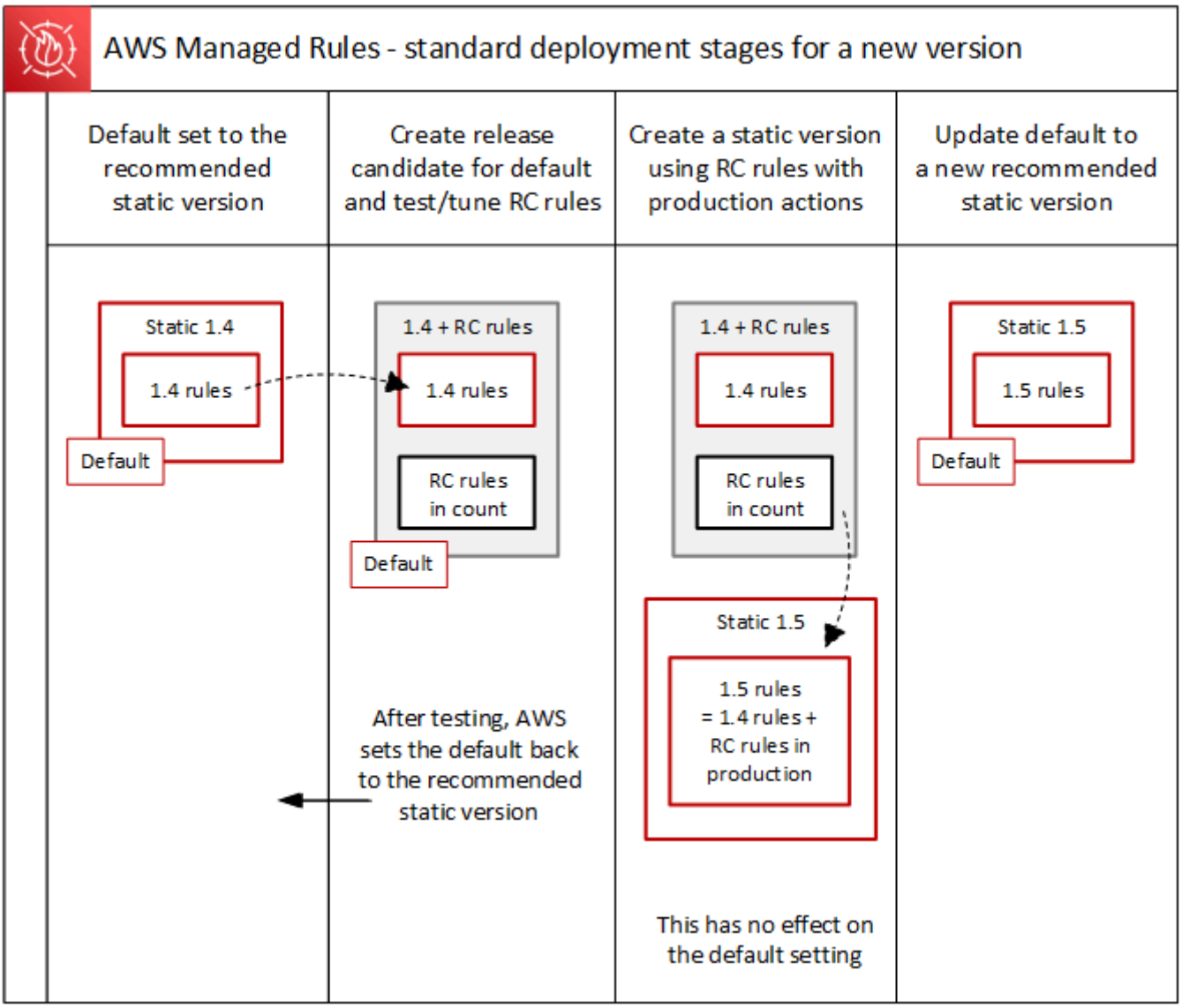
de règles géré auquel la notification est destinée. Voici un exemple de liste de notifications pour`AWSManagedRulesCommonRuleSet`.

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

Vue d'ensemble des déploiements standard pour les règles AWS gérées

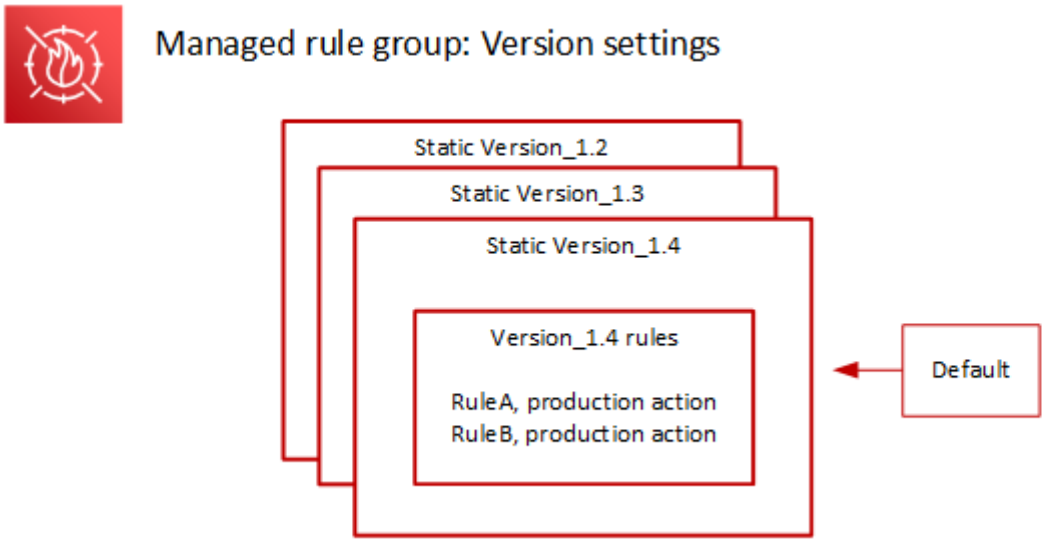
AWS déploie de nouvelles fonctionnalités de règles AWS gérées en trois étapes de déploiement standard : version candidate, version statique et version par défaut.

Le schéma suivant décrit ces déploiements standard. Chacune est décrite plus en détail dans les sections qui suivent.



États de version typiques pour les règles AWS gérées

Normalement, un groupe de règles géré versionné possède un certain nombre de versions statiques non expirées, et la version par défaut pointe vers la version statique recommandée. AWS La figure suivante montre un exemple d'ensemble typique de versions statiques et de paramètres de version par défaut.



L'action de production pour la plupart des règles d'une version statique l'estBlock, mais elle peut être définie différemment. Pour des informations détaillées sur les paramètres d'action des règles, consultez la liste des règles pour chaque groupe de règles à l'adresseAWS Liste des groupes de règles gérées.

Publiez des déploiements candidats pour AWS Managed Rules

Lorsqu'un ensemble de règles candidat AWS est modifié pour un groupe de règles géré, il les teste dans le cadre d'un déploiement de version temporaire candidate. AWS évalue les règles candidates en mode comptage par rapport au trafic de production et effectue les dernières activités de réglage, notamment en atténuant les faux positifs. AWS les tests publient les règles candidates de cette manière pour tous les clients qui utilisent la version par défaut du groupe de règles. Les déploiements de versions candidates ne s'appliquent pas aux clients qui utilisent une version statique du groupe de règles.

Si vous utilisez la version par défaut, le déploiement d'une version candidate ne modifiera pas la façon dont votre trafic Web est géré par le groupe de règles. Vous remarquerez peut-être ce qui suit lors du test des règles relatives aux candidats :

- Le nom de version par défaut passe de `Default (using Version_X.Y)` à`Default (using Version_X.Y_PLUS_RC_COUNT)`.
- Indicateurs de comptage supplémentaires sur Amazon CloudWatch avec leur nom `RC_COUNT` dans leur nom. Elles sont générées par les règles des versions candidates.

AWS teste une version candidate pendant environ une semaine, puis la supprime et rétablit la version par défaut sur la version statique actuellement recommandée.

AWS exécute les étapes suivantes pour le déploiement d'une version candidate :

1. Créer la version candidate : AWS ajoute une version candidate en fonction de la version statique actuellement recommandée, qui est la version vers laquelle pointe la version par défaut.

   Le nom de la version candidate est le nom de version statique auquel est ajouté. `_PLUS_RC_COUNT` Par exemple, si la version statique actuellement recommandée est la version statique`Version_2.1`, la version candidate sera nommée`Version_2.1_PLUS_RC_COUNT`.

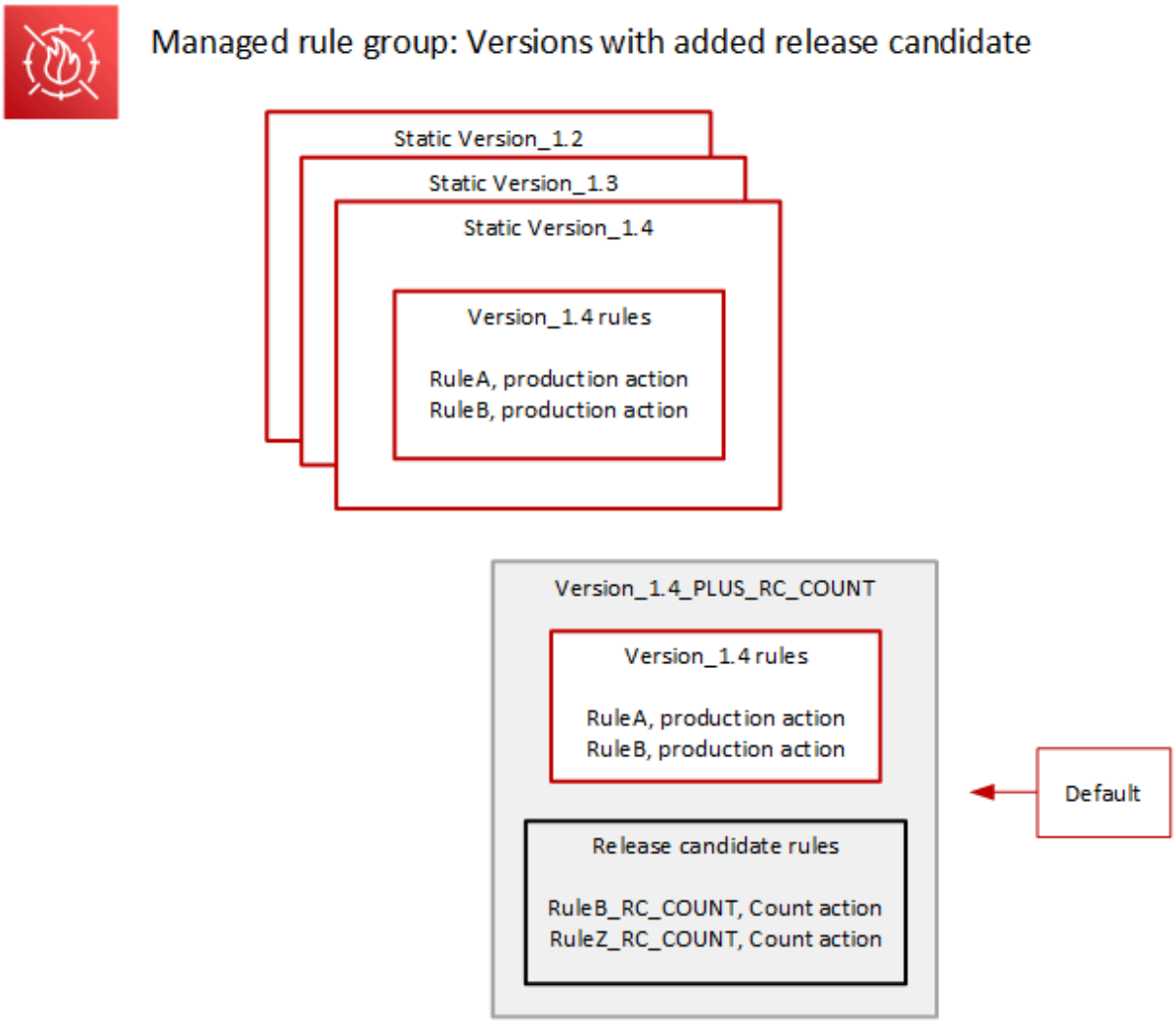
   La version candidate contient les règles suivantes :

   - Règles copiées exactement à partir de la version statique actuellement recommandée, sans modification de la configuration des règles.
   - Nouvelles règles candidates dont l'action est définie sur Count et dont les noms se terminent par`_RC_COUNT`.

     La plupart des règles candidates proposent des améliorations aux règles qui existent déjà dans le groupe de règles. Le nom de chacune de ces règles est le nom de la règle existante auquel est ajouté. `_RC_COUNT`
2. Définissez la version par défaut sur la version candidate et testez : AWS définit la version par défaut pour qu'elle pointe vers la nouvelle version candidate, afin d'effectuer des tests par rapport à votre trafic de production. Les tests prennent généralement environ une semaine.

   Vous verrez le nom de la version par défaut passer de celui qui indique uniquement la version statique, par exemple`Default (using Version_1.4)`, à un nom qui indique la version statique plus les règles relatives aux versions candidates, telles que`Default (using Version_1.4_PLUS_RC_COUNT)`. Ce schéma de dénomination vous permet d'identifier la version statique que vous utilisez pour gérer votre trafic Web.

   Le schéma suivant montre l'état des exemples de versions de groupes de règles à ce stade.



Les règles des versions candidates sont toujours configurées avec des Count actions, de sorte qu'elles ne modifient pas la façon dont le groupe de règles gère le trafic Web.

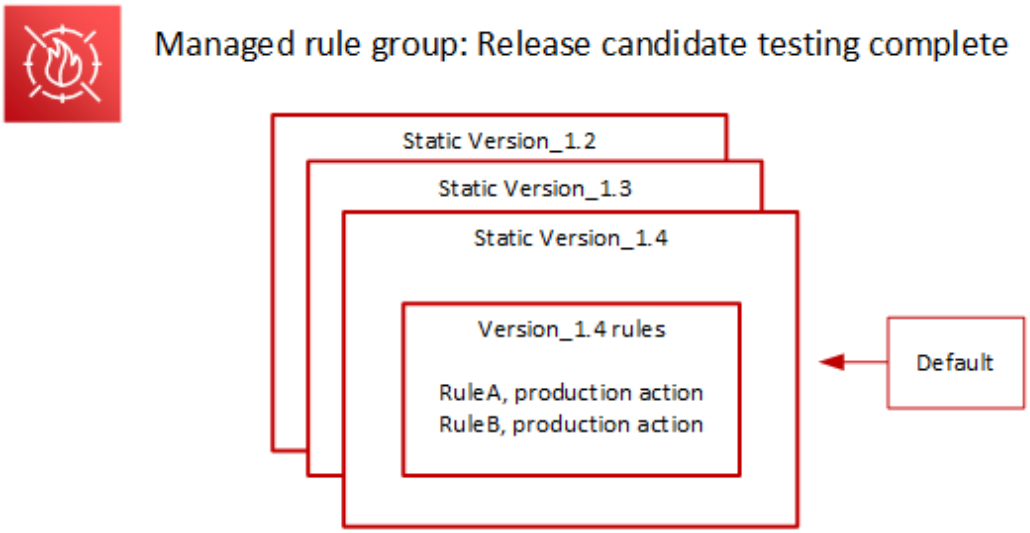
Les règles relatives aux versions candidates génèrent des indicateurs de CloudWatch comptage Amazon qui sont AWS utilisés pour vérifier le comportement et identifier les faux positifs. AWS effectue les ajustements nécessaires, pour ajuster le comportement des règles de dénombrement des candidats à la publication.

La version candidate n'est pas une version statique et vous ne pouvez pas la choisir dans la liste des versions de groupes de règles statiques. Vous pouvez uniquement voir le nom de la version candidate dans la spécification de version par défaut.

3. Rétablir la version par défaut à la version statique recommandée : après avoir testé les règles de la version candidate AWS , rétablit la version par défaut sur la version statique recommandée actuelle. Le paramètre de nom de version par défaut supprime la `_PLUS_RC_COUNT` fin et le

groupe de règles arrête de générer des mesures de CloudWatch nombre pour les règles des versions candidates. Il s'agit d'une modification silencieuse, différente du déploiement d'une restauration de version par défaut.

Le schéma suivant montre l'état des exemples de versions de groupes de règles une fois le test de la version candidate terminé.



Chronométrage et notifications

AWS déploie les versions candidates selon les besoins, afin de tester les améliorations apportées à un groupe de règles.

- SNS — AWS envoie une notification SNS au début du déploiement. La notification indique la durée estimée pendant laquelle la version candidate sera testée. Lorsque le test est terminé, AWS rétablit silencieusement le paramètre de version statique par défaut, sans autre notification.
- Journal des modifications : AWS ne met pas à jour le journal des modifications ni les autres parties de ce guide pour ce type de déploiement.

Déploiements de versions statiques pour les règles AWS gérées

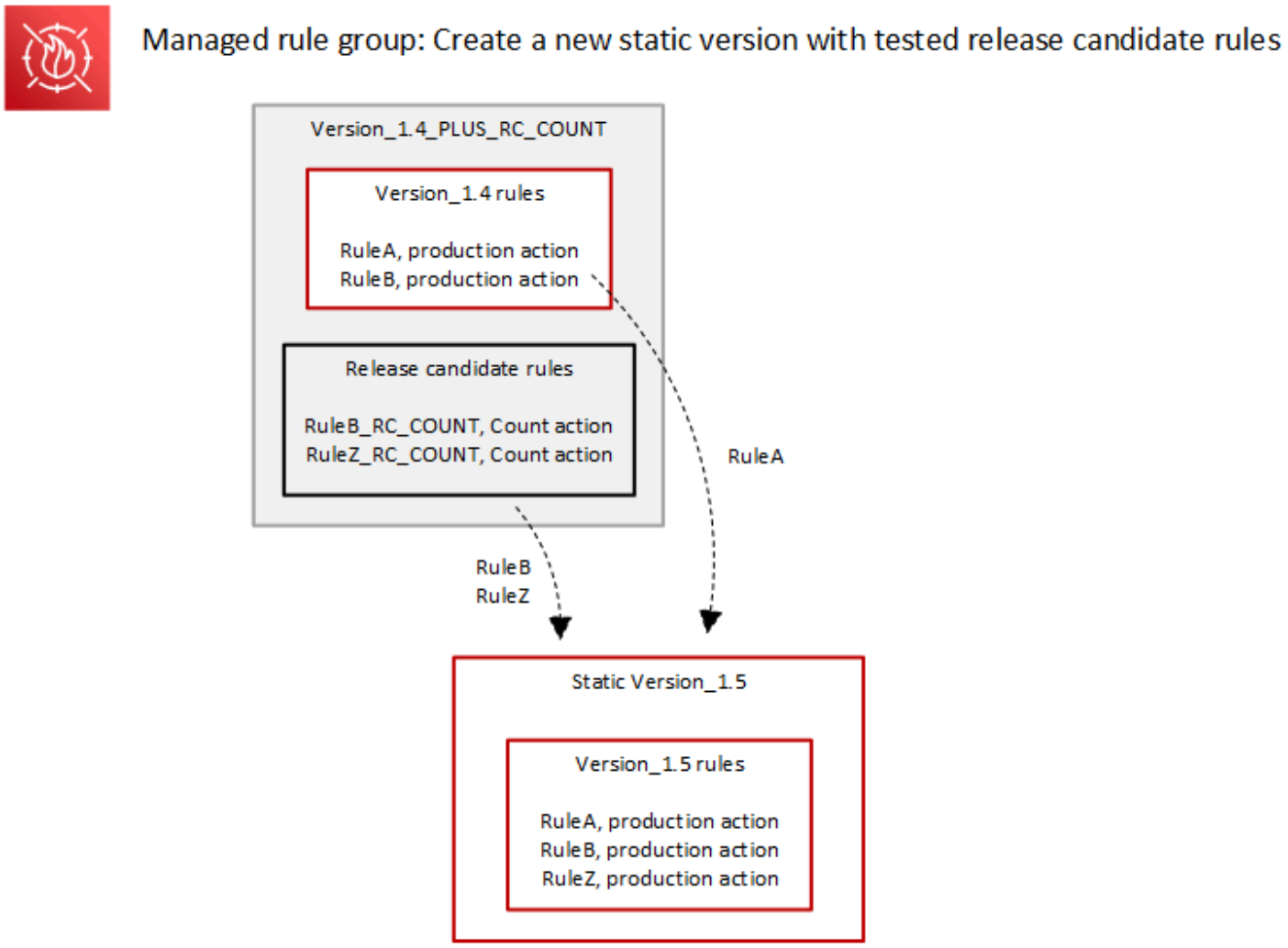
Lorsqu'il est AWS déterminé qu'une version candidate apporte des modifications importantes au groupe de règles, AWS déploie une nouvelle version statique pour le groupe de règles en fonction de la version candidate. Ce déploiement ne modifie pas la version par défaut du groupe de règles.

La nouvelle version statique contient les règles suivantes issues de la version candidate :

- Règles issues de la version statique précédente qui n'ont pas de candidat de remplacement parmi les règles des versions candidates.
- Publiez les règles relatives aux candidats, avec les modifications suivantes :
  - AWS modifie le nom de la règle en supprimant le suffixe `_RC_COUNT` de la version candidate.
  - AWS remplace les actions de règle par Count leurs actions de règles de production.

  Pour les règles candidates qui remplacent des règles existantes, cela remplace les fonctionnalités des règles précédentes dans la nouvelle version statique.

Le schéma suivant illustre la création de la nouvelle version statique à partir de la version candidate.



Après le déploiement, la nouvelle version statique est disponible pour que vous puissiez la tester et l'utiliser dans vos protections si vous le souhaitez. Vous pouvez consulter les actions et les

descriptions des règles nouvelles et mises à jour dans les listes de règles du groupe de règles à l'adresseAWS Liste des groupes de règles gérées.

Une version statique est immuable après le déploiement et ne change que lorsqu'elle AWS expire. Pour plus d'informations sur les cycles de vie des versions, consultezGroupes de règles gérés versionnés.

Chronométrage et notifications

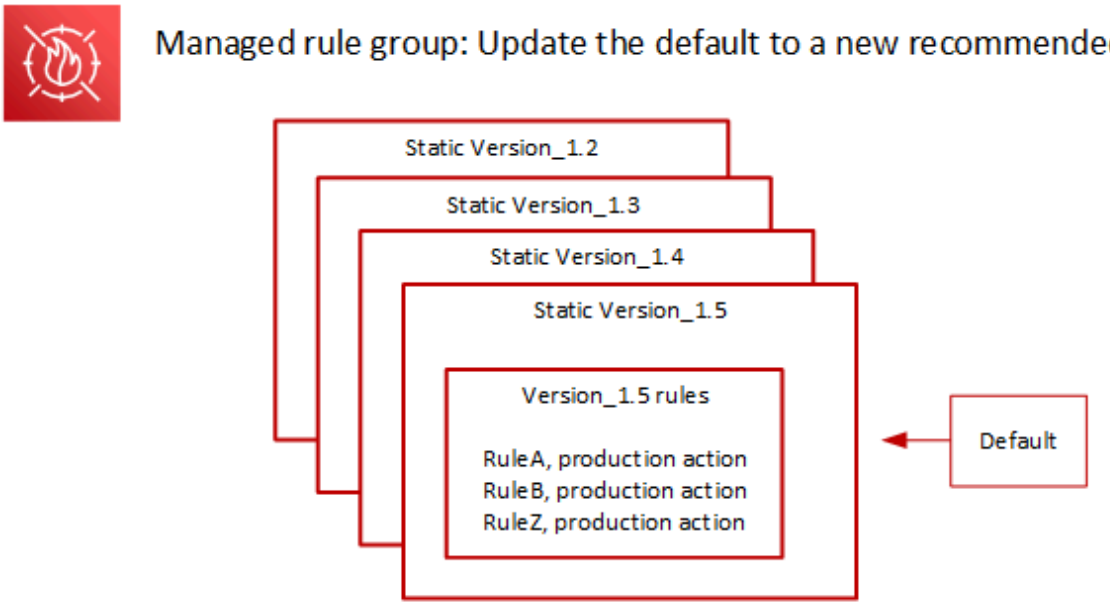
AWS déploie une nouvelle version statique selon les besoins, afin de déployer des améliorations aux fonctionnalités des groupes de règles. Le déploiement d'une version statique n'a aucune incidence sur le paramètre de version par défaut.

- SNS — AWS envoie une notification SNS lorsque le déploiement est terminé.
- Journal des modifications : une fois le déploiement terminé partout où cela AWS WAF est disponible, AWS met à jour la définition du groupe de règles dans ce guide selon les besoins, puis annonce la publication dans le journal des modifications du groupe de règles AWS Managed Rules et sur la page d'historique de la documentation.

Déploiements de versions par défaut pour AWS Managed Rules

Lorsqu'il est AWS déterminé qu'une nouvelle version statique fournit une meilleure protection au groupe de règles par rapport à la version par défaut actuelle, AWS met à jour la version par défaut vers la nouvelle version statique. AWS peut publier plusieurs versions statiques avant de promouvoir l'une d'entre elles vers la version par défaut du groupe de règles.

Le schéma suivant montre l'état des exemples de versions de groupes de règles après le AWS déplacement du paramètre de version par défaut vers la nouvelle version statique.



Avant de déployer cette modification dans la version par défaut, AWS fournit des notifications afin que vous puissiez tester et préparer les modifications à venir. Si vous utilisez la version par défaut, vous ne pouvez effectuer aucune action et y rester pendant toute la durée de la mise à jour. Si vous souhaitez plutôt retarder le passage à la nouvelle version, avant le début prévu du déploiement de la version par défaut, vous pouvez configurer explicitement votre groupe de règles pour qu'il utilise la version statique définie par défaut.

Chronométrage et notifications

AWS met à jour la version par défaut lorsqu'il recommande une version statique différente de celle actuellement utilisée pour le groupe de règles.

- SNS : AWS envoie une notification SNS au moins une semaine avant le jour de déploiement ciblé, puis une autre le jour du déploiement, au début du déploiement. Chaque notification inclut le nom du groupe de règles, la version statique vers laquelle la version par défaut est mise à jour, la date de déploiement et le calendrier prévu du déploiement pour chaque AWS région dans laquelle la mise à jour est effectuée.
- Journal des modifications : AWS ne met pas à jour le journal des modifications ni les autres parties de ce guide pour ce type de déploiement.

Déploiements exceptionnels pour les règles AWS gérées

AWS peut contourner les étapes de déploiement standard afin de déployer rapidement les mises à jour qui répondent aux risques de sécurité critiques. Un déploiement exceptionnel peut impliquer l'un des types de déploiement standard, et il peut être déployé rapidement dans les AWS régions.

AWS fournit une notification aussi avancée que possible pour les déploiements d'exceptions.

Calendrier et notifications

AWS effectue des déploiements d'exceptions uniquement lorsque cela est nécessaire.

- SNS : AWS envoie une notification SNS aussi longtemps que possible avant le jour de déploiement ciblé, puis une autre au début du déploiement. Chaque notification inclut le nom du groupe de règles, les modifications apportées et la date de déploiement.
- Journal des modifications : si le déploiement concerne une version statique, une fois le déploiement terminé partout où cela AWS WAF est disponible, AWS met à jour la définition du groupe de règles dans ce guide selon les besoins, puis annonce la publication dans le journal des modifications du groupe de règles AWS gérées et sur la page d'historique de la documentation.

Annulations de déploiement par défaut pour les règles AWS gérées

Dans certaines conditions, AWS peut rétablir les paramètres précédents de la version par défaut. Une annulation prend généralement moins de dix minutes pour toutes les AWS régions.

AWS effectue une annulation uniquement pour atténuer un problème important dans une version statique, tel qu'un niveau inacceptable de faux positifs.

Après l'annulation du paramètre de version par défaut, AWS accélère à la fois l'expiration de la version statique présentant le problème et la publication d'une nouvelle version statique pour résoudre le problème.

Chronométrage et notifications

AWS effectue des annulations de version par défaut uniquement lorsque cela est nécessaire.

- SNS : AWS envoie une seule notification SNS au moment de l'annulation. La notification inclut le nom du groupe de règles, la version pour laquelle la version par défaut est définie et la date de déploiement. Ce type de déploiement étant très rapide, la notification ne fournit pas d'informations temporelles pour les régions.

- Journal des modifications : AWS ne met pas à jour le journal des modifications ni les autres parties de ce guide pour ce type de déploiement.

AWS Avertissement relatif aux règles gérées

AWS Les règles gérées sont conçues pour vous protéger contre les menaces Web les plus courantes. Lorsqu'ils sont utilisés conformément à la documentation, les groupes de règles AWS gérées ajoutent un niveau de sécurité supplémentaire à vos applications. Cependant, les groupes de règles AWS gérées ne sont pas destinés à remplacer vos responsabilités en matière de sécurité, qui sont déterminées par les AWS ressources que vous sélectionnez. Reportez-vous au modèle de responsabilité partagée pour vous assurer que vos ressources AWS sont correctement protégées.

AWS Journal des modifications des règles gérées

Cette section répertorie les modifications apportées aux règles AWS gérées AWS WAF depuis leur publication en novembre 2019.

> **Note**
>
> Ce journal des modifications indique les modifications apportées aux règles et aux groupes de règles dans AWS Managed Rules for. AWS WAF
> Pour leGroupes de règles de réputation IP, ce journal des modifications indique les modifications apportées aux règles et au groupe de règles, ainsi que les modifications importantes apportées aux sources des listes d'adresses IP utilisées par les règles. Il ne signale pas les modifications apportées aux listes d'adresses IP elles-mêmes, en raison de la nature dynamique de ces listes. Si vous avez des questions concernant les listes d'adresses IP, contactez votre responsable de compte ou ouvrez un dossier auprès AWS Support du Center.

Groupe de règles et règles	Description	Date
Groupe de règles géré par le système d'exploitation Linux Toutes les règles	A publié la version statique 2.3 de ce groupe de règles. Cela ne modifie pas le paramètre de version par défaut.	06/06/2024

Groupe de règles et règles	Description	Date
	Signatures ajoutées pour améliorer la détection.	
AWS WAF Groupe de règles Bot Control AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP) AWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes	Les groupes de règles relatives aux robots et aux fraudes sont désormais versionnés. Si vous utilisez l'un de ces groupes de règles, cette mise à jour ne modifie pas la façon dont il gère votre trafic Web. Cette mise à jour définit la version actuelle du groupe de règles sur la version statique 1.0 et définit la version par défaut pour qu'elle pointe vers celui-ci. Pour plus d'informations sur les règles gérées versionné es, consultez les rubriques suivantes : • Groupes de règles gérés versionnés • Déploiements pour les groupes de règles AWS gérées versionnés • Être informé des nouvelles versions et des mises à jour d'un groupe de règles géré	29/05/2024

Groupe de règles et règles	Description	Date
Groupe de règles géré par le système d'exploitation POSIX • UNIXShellCommandsVariables_QUERYARGUMENTS • UNIXShellCommandsVariables_QUERYSTRING • UNIXShellCommandsVariables_HEADER • UNIXShellCommandsVariables_BODY	A publié la version statique 3.0 de ce groupe de règles. Cela ne modifie pas le paramètre de version par défaut. UNIXShellCommandsVariables_QUERYARGUMENTS Supprimé et remplacé parUNIXShellCommandsVariables_QUERYSTRING . Si vous avez des règles qui correspondent sur l'étiquette pourUNIXShellCommandsVariables_QUERYARGUMENTS , lorsque vous utiliserez cette version, remplacez-les pour qu'elles correspondent à l'étiquette pourUNIXShellCommandsVariables_QUERYSTRING . Le nouveau label estawswaf:managed:aws:posix-os:UNIXShellCommandsVariables_QueryString . Ajout de la règleUNIXShellCommandsVariables_HEADER , qui correspond à tous les en-têtes. Toutes les règles du groupe de règles géré ont été mises à jour avec une logique de détection améliorée.	28/05/2024

Groupe de règles et règles	Description	Date
	Correction de la capitalisation documentée de l'étiquette pour`UNIXShellCommandsVariables_BODY` .	
Groupe de règles géré par un ensemble de règles de base (CRS) • `CrossSiteScripting*`	A publié la version statique 1.12 de ce groupe de règles. Ajout de signatures à toutes les règles de script intersites afin d'améliorer la détection et de réduire le nombre de faux positifs.	21/05/2021
Groupe de règles géré par base de données SQL • `SQLi_BODY` • `SQLi_QUERYARGUMENTS` • `SQLiExtendedPatterns_QUERYARGUMENTS`	A publié la version statique 1.2 de ce groupe de règles. La transformation de `JS_DECODE` texte a été ajoutée aux règles répertoriées.	14/05/2024
Groupe de règles géré pour les entrées erronées connues • `JavaDeserializationRCE_BODY` • `JavaDeserializationRCE_QUERYSTRING` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_BODY` • `Log4JRCE_HEADER`	A publié la version statique 1.22 de ce groupe de règles. La transformation de `JS_DECODE` texte a été ajoutée aux règles répertoriées.	08-05-2024/

Groupe de règles et règles	Description	Date
Groupe de règles géré par le système d'exploitation POSIX	A publié la version statique 2.2 de ce groupe de règles. La transformation du `JS_DECODE` texte a été ajoutée aux deux règles.	08-05-2024/
Groupe de règles géré par le système d'exploitation Windows • `PowerShellCommands_BODY`	A publié la version statique 2.1 de ce groupe de règles. Ajout de signatures `PowerShellCommands_BODY` pour améliorer la détection.	03/05/2024
Groupe de règles géré par Amazon IP Reputation • `AWSManagedIPReputationList`	Mise à jour des sources de la liste de réputation des adresses IP, afin d'améliorer l'identification des adresses activement impliquées dans des activités malveillantes et de réduire le nombre de faux positifs. Cette mise à jour n'implique pas de nouvelle version car ce groupe de règles n'est pas versionné.	13/03/2024
Groupe de règles géré pour les entrées erronées connues	A publié la version statique 1.21 de ce groupe de règles. Ajout de signatures pour améliorer la détection et réduire le nombre de faux positifs.	16/12/2023

Groupe de règles et règles	Description	Date
Groupe de règles géré pour les entrées erronées connues • `ExploitablePaths_URIPATH`	A publié la version statique 1.20 de ce groupe de règles. Mise à jour de la `ExploitablePaths_URIPATH` règle afin d'ajouter la détection des demandes correspondant à la vulnérabilité d'autorisation incorrecte CVE-2023-22518 d'Atlassian Confluence. Cette vulnérabilité affecte toutes les versions de Confluence Data Center et Server. Pour plus d'informations, voir NIST : National Vulnerability Database : CVE-2023-22518 Detail.	14/12/2023
Groupe de règles géré par un ensemble de règles de base (CRS) • `CrossSiteScripting*`	A publié la version statique 1.11 de ce groupe de règles. Ajout de signatures à toutes les règles de script intersites afin d'améliorer la détection et de réduire le nombre de faux positifs.	06/12/2023

Groupe de règles et règles	Description	Date
AWS WAF Groupe de règles Bot Control • Nouveau label : `awswaf:managed:aws:bot-control:targeted:aggregate:coordinated_activity:low`	L'étiquette « faible activité coordonnée » a été ajoutée aux étiquettes de niveau de protection ciblées du groupe de règles. Cette étiquette n'est associée à aucune règle. Cet étiquetage s'ajoute aux règles et labels de niveau moyen et élevé.	23/12-05
Étiquettes Bot Control • Libellé : `awswaf:managed:aws:bot-control:targeted:signal:browser_automation_extension`	Ajout d'une étiquette de signal au groupe de règles indiquant la détection d'une extension de navigateur facilitant l'automatisation. Cette étiquette n'est pas spécifique à une règle individuelle.	14/11/2023
Groupe de règles géré par un ensemble de règles de base (CRS) • `EC2MetaDataSSRF_QUERYARGUMENTS`	A publié la version statique 1.10 de ce groupe de règles. Mise à jour d'une règle pour améliorer la détection et réduire le nombre de faux positifs.	02/11/2023

Groupe de règles et règles	Description	Date
Groupe de règles géré par un ensemble de règles de base (CRS) • `EC2MetaDataSSRF_BODY` • `EC2MetaDataSSRF_COOKIE` • `EC2MetaDataSSRF_URIPATH` • `EC2MetaDataSSRF_QUERYARGUMENTS`	A publié la version statique 1.9 de ce groupe de règles. Règles mises à jour pour améliorer la détection et réduire les faux positifs.	30/10/2023
Groupe de règles géré par le système d'exploitation POSIX • `UNIXShellCommandsVariables_QUERYARGUMENTS`	A publié la version statique 2.1 de ce groupe de règles. Mise à jour de la règle des arguments de requête pour améliorer la détection.	2023-10-12

Groupe de règles et règles	Description	Date
Groupe de règles géré par un ensemble de règles de base (CRS) • `GenericLFI_QUERYARGUMENTS` • `GenericLFI_URIPATH` • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS`	A publié la version statique 1.8 de ce groupe de règles. Règles mises à jour pour améliorer la détection.	11/10/2023

Groupe de règles et règles	Description	Date
Groupe de règles géré pour les entrées erronées connues • `ExploitablePaths_URIPATH`	Déploiement exceptionnel : publication de la version statique 1.19 de ce groupe de règles. Mise à jour de la version par défaut pour utiliser la version 1.19. Mise à jour de la `ExploitablePaths_URIPATH` règle afin d'ajouter la détection des demandes correspondant à la vulnérabilité d'escalade de privilèges CVE-2023-22515 d'Atlassian Confluence. Cette vulnérabilité affecte certaines versions d'Atlassian Confluence. Pour plus d'informations, consultez NIST : National Vulnerability Database : CVE-2023-22515 Detail et Atlassian Support : FAQ pour CVE-2023-22515. Pour plus d'informations sur ce type de déploiement, consultezDéploiements exceptionnels pour les règles AWS gérées.	04/10/2023

Groupe de règles et règles	Description	Date
Groupe de règles géré pour les entrées erronées connues • `Host_localhost_HEADER` • `Log4J*` • `JavaDeserialization*`	Déploiement exceptionnel : publication de la version statique 1.18 de ce groupe de règles. Il s'agit d'un déploiement rapide de cette version statique pour permettre la création et le déploiement de la version 1.19. Mise à jour de la `Host_localhost_HEADER` règle et de toutes les règles de désérialisation de Log4J et Java pour une meilleure détection. Pour plus d'informations sur ce type de déploiement, consultezDéploiements exceptionnels pour les règles AWS gérées.	04/10/2023

Groupe de règles et règles	Description	Date
AWS WAF Groupe de règles Bot Control • `TGT_TokenReuseIp` • `TGT_ML_CoordinatedActivityMedium` • `TGT_ML_CoordinatedActivityHigh`	Des règles ont été ajoutées au groupe de règles avec Count action. La règle IP de réutilisation des jetons détecte et compte le partage de jetons entre les adresses IP. Les règles d'activité coordonnées utilisent une analyse automatisée basée sur l'apprentissage automatiq ue (ML) du trafic du site Web pour détecter les activités liées aux robots. Dans la configuration de votre groupe de règles, vous pouvez refuser l'utilisation du ML. Avec cette version, les clients qui utilisent actuellement le niveau de protection ciblé ont opté pour l'utilisation du ML. La désinscri ption désactive les règles d'activité coordonnées.	06/09/2023
AWS WAF Groupe de règles Bot Control • `CategoryAI`	La règle a été ajoutée `CategoryAI` au groupe de règles.	30/08/2023

Groupe de règles et règles	Description	Date
Groupe de règles géré par un ensemble de règles de base (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS` • `EC2MetaDataSSRF_COOKIE` • `EC2MetaDataSSRF_QUERYARGUMENTS` • `EC2MetaDataSSRF_BODY` • `EC2MetaDataSSRF_URIPATH`	A publié la version statique 1.7 de ce groupe de règles. Extensions restreintes mises à jour et règles SSRF des métadonnées EC2 pour améliorer la détection et réduire les faux positifs.	26/07/2023
AWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes Toutes les règles du nouveau groupe de règles	Le groupe de règles a été ajouté`AWSManagedRulesACFPRuleSet` .	13/06/2023

Groupe de règles et règles	Description	Date
Groupe de règles géré par le système d'exploitation Linux • LFI_HEADER • LFI_URIPATH • LFI_QUERYSTRING	A publié la version statique 2.2 de ce groupe de règles. Signatures ajoutées pour améliorer la détection.	22/05/2023
Groupe de règles géré par un ensemble de règles de base (CRS) • RestrictedExtensions_URIPATH • RestrictedExtensions_QUERYARGUMENTS • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	A publié la version statique 1.6 de ce groupe de règles. Mise à jour du cross-site scripting (XSS) et règles d'extension restreintes pour améliorer la détection et réduire les faux positifs.	28/04/2023

Groupe de règles et règles	Description	Date
Groupe de règles géré par une application PHP • Mise à jour d'PHPHighRiskMethodsVariables_BODY • Supprimé PHPHighRiskMethodsVariables_QUERYARGUMENTS • Ajout de PHPHighRiskMethodsVariables_QUERYSTRING . • Ajout de PHPHighRiskMethodsVariables_HEADER .	A publié la version statique 2.0 de ce groupe de règles. Signatures ajoutées pour améliorer la détection dans toutes les règles. La règle PHPHighRiskMethodsVariables_QUERYARGUMENTS a été remplacée parPHPHighRiskMethodsVariables_QUERYSTRING , qui inspecte l'intégralité de la chaîne de requête au lieu de se limiter aux arguments de la requête. Ajout de la règlePHPHighRiskMethodsVariables_HEADER , pour étendre la couverture afin d'inclure tous les en-têtes. Les libellés suivants ont été mis à jour pour les aligner sur l'étiquetage standard des règles AWS gérées : • Ancien nom : PHPHighRiskMethodsVariables_BODY Nouveau nom : PHPHighRiskMethodsVariables_Body • Ancien nom : PHPHighRiskMethodsVariables	27/02/2023

Groupe de règles et règles	Description	Date
	`_QUERYARGUMENTS` Nouveau nom : `PHPHighRiskMethodsVariables_QueryString`	
AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP) • `VolumetricIpFailedLoginResponseHigh` • `VolumetricSessionFailedLoginResponseHigh`	Ajout de règles d'inspection des réponses de connexion à utiliser avec les CloudFront distributions Amazon protégées. Ces règles peuvent bloquer les nouvelles tentatives de connexion provenant d'adresses IP et de sessions client qui ont récemment été à l'origine d'un trop grand nombre de tentatives de connexion infructueuses.	15/02/2023
Groupe de règles géré par un ensemble de règles de base (CRS) • `NoUserAgent_HEADER` • `CrossSiteScripting_COOKIE` • `CrossSiteScripting_QUERYARGUMENTS` • `CrossSiteScripting_BODY` • `CrossSiteScripting_URIPATH`	A publié la version statique 1.5 de ce groupe de règles. Filtres XSS (Cross Site Scripting) mis à jour pour améliorer la détection.	25/01/2023

Groupe de règles et règles	Description	Date
Groupe de règles géré par le système d'exploitation Linux • `LFI_COOKIE` - retiré • `LFI_HEADER` - ajouté • `LFI_URIPATH` • `LFI_QUERYSTRING`	A publié la version statique 2.1 de ce groupe de règles. Suppression de la règle `LFI_COOKIE` et de son étiquette`awswaf:managed:aws:linux-os:LFI_Cookie`, et remplacée par la nouvelle règle `LFI_HEADER` et son étiquette`awswaf:managed:aws:linux-os:LFI_Header`. Cette modification étend l'inspection à plusieurs en-têtes. Des transformations de texte et des signatures ont été ajoutées à toutes les règles pour améliorer la détection.	15 décembre

Groupe de règles et règles	Description	Date
Groupe de règles géré par un ensemble de règles de base (CRS) • NoUserAgent_HEADER • CrossSiteScripting_COOKIE • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_BODY • CrossSiteScripting_URIPATH	A publié la version statique 1.4 de ce groupe de règles. Ajout d'une transformation de texte NoUserAgent_HEADER pour supprimer tous les octets nuls. Mise à jour des filtres dans les règles de script intersite afin d'améliorer la détection.	05.12-05

Groupe de règles et règles	Description	Date
Groupe de règles géré pour les entrées erronées connues • `JavaDeserializationRCE_BODY` • `JavaDeserializationRCE_URIPATH` • `JavaDeserializationRCE_HEADER` • `JavaDeserializationRCE_QUERYSTRING` • `Host_localhost_HEADER`	A publié la version statique 1.17 de ce groupe de règles. Mise à jour des règles de désérialisation de Java afin d'ajouter la détection des requêtes correspondant à Apache CVE-42889, une vulnérabilité d'exécution de code à distance (RCE) dans les versions d'Apache Commons Text antérieur es à la version 1.10.0. Pour plus d'informations, consultez NIST : National Vulnerability Database : CVE-42889 Detail et CVE-42889 : Apache Commons Text antérieur à la version 1.10.0 autorise le RCE lorsqu'il est appliqué à des entrées non fiables en raison de valeurs d'interpolation par défaut non sécurisées. Détection améliorée dans`Host_localhost_HEADER` .	10-20

Groupe de règles et règles	Description	Date
Groupe de règles géré pour les entrées erronées connues • `Log4JRCE_HEADER` • `Log4JRCE_QUERYSTRING` • `Log4JRCE_URIPATH` • `Log4JRCE_BODY`	A publié la version statique 1.16 de ce groupe de règles. Suppression des faux positifs AWS identifiés dans la version 1.15.	05.10-05
Groupe de règles géré par le système d'exploitation POSIX Groupe de règles géré par une application PHP WordPress groupe de règles géré par les applications	Les noms d'étiquettes documentés ont été corrigés.	09-19
Groupes de règles de réputation IP • `AWSManagedIPDDoSList`	Cette modification ne modifie pas la façon dont le groupe de règles gère le trafic Web. Ajout d'une nouvelle règle Count permettant d'inspecter les adresses IP activement impliquées dans des activités DDoS, selon Amazon Threat Intelligence.	08-30

Groupe de règles et règles	Description	Date
Groupe de règles géré pour les entrées erronées connues • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URIPATH • Log4JRCE_BODY • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URIPATH • JavaDeserializationRCE_QUERYSTRING • Host_localhost_HEADER • PROPFIND_METHOD	A publié la version statique 1.15 de ce groupe de règles. Log4JRCESupprimé et remplacé parLog4JRCE_HEADER ,Log4JRCE_QUERYSTRING , et Log4JRCE_URI Log4JRCE_BODY , pour une surveillance et une gestion plus précises des faux positifs. Des signatures ont été ajoutées pour améliorer la détection et le blocage de tous PROPFIND_METHOD JavaDeserializationRCE* et de toutes les Log4JRCE* règles. Libellés mis à jour pour corriger la capitalisation dans Host_localhost_HEADER et dans toutes les JavaDeserializationRCE* règles. Corrigé la description deJavaDeserializationRCE_HEADER .	22/08

Groupe de règles et règles	Description	Date
AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP) • `UnsupportedCognitoIDP`	Ajout d'une règle pour empêcher l'utilisation du groupe de règles géré de prévention du piratage de compte pour le trafic Web du groupe d'utilisateurs Amazon Cognito.	08-11
Groupe de règles géré par un ensemble de règles de base (CRS)	AWS a une date d'expiration planifiée pour les versions `Version_1.2` et pour le groupe `Version_2.0` de règles. Les versions expireront le 9 septembre 2022. Pour plus d'informations sur l'expiration des versions, consultez Groupes de règles gérés versionnés.	09/06/2018
Groupe de règles géré par un ensemble de règles de base (CRS) • `GenericLFI_URIPATH` `GenericRFI_URIPATH`	A publié la version 1.3 de ce groupe de règles. Cette version met à jour les signatures de correspondance dans les règles `GenericLFI_URIPATH` et`GenericRFI_URIPATH`, pour améliorer la détection.	24/05/2018
AWS WAF Groupe de règles Bot Control • `CategoryEmailClient`	La règle a été ajoutée `CategoryEmailClient` au groupe de règles.	06/04/2018

Groupe de règles et règles	Description	Date
Groupe de règles géré pour les entrées erronées connues • JavaDeserializationRCE_HEADER • JavaDeserializationRCE_BODY • JavaDeserializationRCE_URI • JavaDeserializationRCE_QUERYSTRING	A publié la version 1.14 de ce groupe de règles. Les quatre JavaDeseriallztion RCE règles passent en Block mode.	31 mars
Groupe de règles géré pour les entrées erronées connues • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT	A publié la version 1.13 de ce groupe de règles. Mise à jour de la transformation de texte pour les vulnérabilités Spring Core et Cloud Function RCE. Ces règles sont en mode décompte pour recueillir des métriques et évaluer les modèles correspondants. L'étiquette peut être utilisée pour bloquer les demandes dans une règle personnalisée. Une version ultérieure sera déployée avec ces règles en mode bloc.	31 mars

Groupe de règles et règles	Description	Date
Groupe de règles géré pour les entrées erronées connues • JavaDeserializationRCE_HEADER_RC_COUNT • JavaDeserializationRCE_BODY_RC_COUNT • JavaDeserializationRCE_URI_RC_COUNT • JavaDeserializationRCE_QUERYSTRING_RC_COUNT • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY • Log4JRCE	A publié la version 1.12 de ce groupe de règles. Signatures ajoutées pour les vulnérabilités Spring Core et Cloud Function RCE. Ces règles sont en mode décompte pour recueillir des métriques et évaluer les modèles correspondants. L'étiquette peut être utilisée pour bloquer les demandes dans une règle personnalisée. Une version ultérieure sera déployée avec ces règles en mode bloc. Suppression des règles Log4JRCE_HEADER Log4JRCE_QUERYSTRING ,Log4JRCE_URI , Log4JRCE_BODY et et remplacées par la règleLog4JRCE.	30/03/2018
Groupes de règles de réputation IP • AWSManagedReconnaissanceList	La AWSManagedReconnaissanceList règle a été mise à jour pour changer l'action du nombre à l'action en bloquant.	15 février

Groupe de règles et règles	Description	Date
AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP) Toutes les règles du nouveau groupe de règles	Le groupe de règles a été ajoutéAWSManagedRulesATPRuleSet .	11 février
Groupe de règles géré pour les entrées erronées connues • Log4JRCE • Log4JRCE_HEADER • Log4JRCE_QUERYSTRING • Log4JRCE_URI • Log4JRCE_BODY	A publié la version 1.9 de ce groupe de règles. Suppression de la règle Log4JRCE et remplacée par les règlesLog4JRCE_HEADER ,Log4JRCE_QUERYSTRING ,Log4JRCE_URI , etLog4JRCE_BODY , pour plus de flexibilité dans l'utilisation de cette fonctionnalité. Signatures ajoutées pour améliorer la détection et le blocage.	28/01/2018
Ensemble de règles de base (CRS) • CrossSiteScripting_URIPATH • CrossSiteScripting_BODY • CrossSiteScripting_QUERYARGUMENTS • CrossSiteScripting_COOKIE	A publié la version 2.0 de ce groupe de règles. Pour ces règles, les signatures de détection ont été ajustées afin de réduire le nombre de faux positifs. La transformation de URL_DECODE texte a été remplacée par la transformation de URL_DECODE_UNI texte double. Ajout de la transformation HTML_ENTITY_DECODE du texte.	01/01/10

Groupe de règles et règles	Description	Date
Ensemble de règles de base (CRS) • `RestrictedExtensions_URIPATH` • `RestrictedExtensions_QUERYARGUMENTS`	Dans le cadre de la publication de la version 2.0 de ce groupe de règles, la transformation du `URL_DECODE_UNI` texte a été ajoutée. Suppression de la transformation de `URL_DECODE` texte de`RestrictedExtensions_URIPATH` .	01/01/10
Base de données SQL • `SQLi_BODY` • `SQLi_QUERYARGUMENTS` • `SQLi_COOKIE` • `SQLi_URIPATH` • `SQLiExtendedPatterns_BODY` • `SQLiExtendedPatterns_QUERYARGUMENTS`	A publié la version 2.0 de ce groupe de règles. La transformation de `URL_DECODE` texte a été remplacée par la transformation de `URL_DECODE_UNI` texte double et la transformation de `COMPRESS_WHITE_SPACE` texte a été ajoutée. Ajout de signatures de détection supplémentaires à`SQLiExtendedPatterns_QUERYARGUMENTS` . L'inspection JSON a été ajoutée à`SQLi_BODY` . La règle a été ajoutée`SQLiExtendedPatterns_BODY` . La règle a été supprimée `SQLi_URIPATH` .	01/01/10

Groupe de règles et règles	Description	Date
Entrées erronées connues • Log4JRCE	Publication de la version 1.8 de la règle Log4JRCE pour améliorer l'inspection des en-têtes et les critères de correspondance.	17/12/2021
Entrées erronées connues • Log4JRCE	Publication de la version 1.4 de la règle Log4JRCE pour ajuster les critères de correspondance et inspecter les en-têtes supplémen taires. Sortie de la version 1.5 pour ajuster les critères de correspondance.	11/12/2021

Groupe de règles et règles	Description	Date
Entrées erronées connues • `Log4JRCE` • `BadAuthToken_COOKIE_AUTHORIZATION`	Ajout de la `Log4JRCE` version 1.2 de la règle en réponse au problème de sécurité récemment révélé dans Log4j. Pour plus d'informations, voir CVE-2021-44228. Cette règle inspecte les chemins d'URI courants, les chaînes de requête, les 8 premiers Ko du corps de la demande et les en-têtes communs. La règle utilise des transformations de `URL_DECODE_UNI` texte double. A publié la version 1.3 de `Log4JRCE` pour ajuster les critères de correspondance et inspecter les en-têtes supplémentaires. La règle a été supprimée `BadAuthToken_COOKIE_AUTHORIZATION` .	2021-12-10

Le tableau suivant répertorie les modifications apportées avant décembre 2021.

Groupe de règles et règles	Description	Date	
Liste de réputation des adresses IP Amazon	`AWSManagedReconnaissanceList`	Ajout de la `AWSManagedReconnaissanceList` règle en mode surveillance/comptage. Cette règle	23/11/2021

Groupe de règles et règles	Description	Date	
		contient les adresses IP qui effectuent une reconnaissance par rapport AWS aux ressources.	

Groupe de règles et règles	Description	Date	
Système d'exploitation Windows	`WindowsShellCommands` `PowerShellCommands`	Ajout de trois nouvelles règles pour WindowsShell les commandes : `WindowsShellCommands_COOKIE` `WindowsShellCommands_QUERYARGUMENTS` , et`WindowsShellCommands_BODY` . Ajout d'une nouvelle PowerShell règle :`PowerShellCommands_COOKIE` . Restructuration de la dénomination `PowerShellComands` des règles en supprimant les chaînes _Set1 et _Set2. Des signatures de détection plus complètes ont été ajoutées	23/11/2021

Groupe de règles et règles	Description	Date	
		àPowerShellRules . Ajout d'une transformation de URL_DECODE_UNI texte à toutes les règles du système d'exploitation Windows.	
Système d'exploitation Linux	LFI_URIPATH LFI_QUERYSTRING LFI_BODY LFI_COOKIE	La transformation de URL_DECODE texte double a été remplacée par une transformation doubleURL_DECODE_UNI . Ajouté NORMALIZE_PATH_WIN en tant que deuxième transformation de texte. A remplacé la LFI_BODY règle par la LFI_COOKIE règle. Ajout de signatures de détection plus complètes pour toutes les LFI règles.	23/11/2021

Groupe de règles et règles	Description	Date	
Ensemble de règles de base (CRS)	`SizeRestrictions_BODY`	Réduction de la limite de taille pour bloquer les requêtes Web dont la charge utile corporelle est supérieure à 8 Ko. Auparavant, la limite était de 10 Ko.	2021-10-27
Ensemble de règles de base (CRS)	`EC2MetaDataSSRF_BODY` `EC2MetaDataSSRF_COOKIE` `EC2MetaDataSSRF_URIPATH` `EC2MetaDataSSRF_QUERYARGUMENTS`	Ajout de nouvelles signatures de détection. Ajout d'un double décodage d'URL Unicode pour améliorer le blocage.	2021-10-27

Groupe de règles et règles	Description	Date	
Ensemble de règles de base (CRS)	`GenericLFI_QUERYARGUMENTS` `GenericLFI_URIPATH` `RestrictedExtensions_URIPATH` `RestrictedExtensions_QUERYARGUMENTS`	Ajout d'un double décodage d'URL Unicode pour améliorer le blocage.	2021-10-27
Ensemble de règles de base (CRS)	`GenericRFI_QUERYARGUMENTS` `GenericRFI_BODY` `GenericRFI_URIPATH`	Mise à jour des signatures de règles afin de réduire le nombre de faux positifs, en fonction des commentaires des clients. Ajout d'un double décodage d'URL Unicode pour améliorer le blocage.	2021-10-27
Tous	Toutes les règles	Ajout de la prise en charge des AWS WAF étiquettes à toutes les règles qui ne prenaient pas déjà en charge l'étiquetage.	2021-10-25

Groupe de règles et règles	Description	Date	
Liste de réputation des adresses IP Amazon	`AWSManagedIPReputationList_xxxx`	Restructuration de la liste de réputation IP, suppression des suffixes du nom de règle et ajout de la prise en charge des étiquettes. AWS WAF	04/05/2021
Liste des adresses IP anonymes	`AnonymousIPList` `HostingProviderList`	Ajout du support pour les AWS WAF étiquettes.	04/05/2021
Contrôle des robots	Tous	Ajout de l'ensemble de règles Bot Control.	01-04-2021
Ensemble de règles de base (CRS)	`GenericRFI_QUERYARGUMENTS`	Ajout d'un double décodage d'URL.	03/03/2021
Ensemble de règles de base (CRS)	`RestrictedExtensions_URIPATH`	Amélioration de la configuration des règles et ajout d'un décodage d'URL supplémentaire.	03/03/2021
Protection de l'administrateur	`AdminProtection_URIPATH`	Ajout d'un double décodage d'URL.	03/03/2021
Entrées erronées connues	`ExploitablePaths_URIPATH`	Amélioration de la configuration des règles et ajout d'un décodage d'URL supplémentaire.	03/03/2021

Groupe de règles et règles	Description	Date	
Système d'exploitation Linux	`LFI_QUERYARGUMENTS`	Amélioration de la configuration des règles et ajout d'un décodage d'URL supplémentaire.	03/03/2021
Système d'exploitation Windows	Tous	Amélioration de la configuration des règles.	2020-09-23
Application PHP	`PHPHighRiskMethodsVariables_QUERYARGUMENTS` `PHPHighRiskMethodsVariables_BODY`	Modification de la transformation du texte du décodage HTML au décodage URL, afin d'améliorer le blocage.	16/09/2020
Système d'exploitation POSIX	`UNIXShellCommandsVariables_QUERYARGUMENTS` `UNIXShellCommandsVariables_BODY`	Modification de la transformation du texte du décodage HTML au décodage URL, afin d'améliorer le blocage.	16/09/2020

Groupe de règles et règles	Description	Date	
Ensemble de règles de base	`GenericLFI_QUERYARGUMENTS` `GenericLFI_URIPATH` GenericLFI_BODY	Modification de la transformation du texte du décodage HTML au décodage URL, afin d'améliorer le blocage.	2020-08-07
Système d'exploitation Linux	`LFI_URIPATH` `LFI_QUERYARGUMENTS` `LFI_BODY`	Changement de la transformation de texte du décodage d'entité HTML au décodage d'URL, afin d'améliorer la détection et le blocage.	19/05/2020
Liste des adresses IP anonymes	Tous	Nouveau groupe de règles visant Groupes de règles de réputation IP à bloquer les demandes provenant de services qui permettent de masquer l'identité des utilisateurs, afin de limiter les robots et de contourner les restrictions géographiques.	06/03/2020
WordPress candidature	`WordPressExploitableCommands_QUERYSTRING`	Nouvelle règle qui vérifie les commandes exploitables dans la chaîne de requête.	03/03/2020

Groupe de règles et règles	Description	Date	
Ensemble de règles de base (CRS)	`SizeRestrictions_QUERYSTRING` `SizeRestrictions_Cookie_HEADER` `SizeRestrictions_BODY` `SizeRestrictions_URIPATH`	Ajustement des contraintes de valeur de taille pour améliorer la précision.	03/03/2020
Base de données SQL	`SQLi_URIPATH`	Les règles vérifient maintenant l'URI du message.	23/01/2020
Base de données SQL	`SQLi_BODY` `SQLi_QUERYARGUMENTS` `SQLi_COOKIE`	Transformations de texte mises à jour.	2019-12-20

Groupe de règles et règles	Description	Date	
Ensemble de règles de base (CRS)	`CrossSite Scripting _URIPATH` `CrossSite Scripting_BODY` `CrossSite Scripting _QUERYARG UMENTS` `CrossSite Scripting _COOKIE`	Transformations de texte mises à jour.	2019-12-20

AWS Marketplace groupes de règles gérés

AWS Marketplace les groupes de règles gérés sont disponibles par abonnement via la AWS Marketplace console à l'adresse AWS Marketplace. Une fois que vous êtes abonné à un groupe de règles AWS Marketplace géré, vous pouvez l'utiliser dans AWS WAF. Pour utiliser un groupe de AWS Marketplace règles dans une AWS Firewall Manager AWS WAF politique, chaque compte de votre organisation doit y souscrire.

Testez et ajustez les modifications apportées à vos AWS WAF protections avant de les utiliser pour le trafic de production. Pour plus d'informations, veuillez consulter Tester et ajuster vos AWS WAF protections.

AWS Marketplace Tarification par groupes de règles

AWS Marketplace les groupes de règles sont disponibles sans contrat à long terme et sans engagement minimum. Lorsque vous vous inscrivez à un groupe de règles, des frais mensuels (au prorata horaire) vous sont facturés, ainsi que des frais basés sur le volume de requêtes en cours. Pour plus d'informations, consultez la section AWS WAF Tarification et la description de chaque groupe de AWS Marketplace règles à l'adresse AWS Marketplace.

Vous avez des questions concernant un groupe de AWS Marketplace règles ?

Pour toute question concernant un groupe de règles géré par un AWS Marketplace vendeur et pour demander des modifications de fonctionnalités, contactez l'équipe du support client du fournisseur. Pour trouver les coordonnées, consultez la liste du fournisseur à l'adresse AWS Marketplace.

Le fournisseur du groupe de AWS Marketplace règles détermine comment gérer le groupe de règles, par exemple comment le mettre à jour et si le groupe de règles est versionné. Le fournisseur détermine également les détails du groupe de règles, notamment les règles, les actions des règles et les étiquettes que les règles ajoutent aux requêtes Web correspondantes.

Abonnement à des groupes de règles AWS Marketplace gérés

Vous pouvez vous abonner à des groupes de AWS Marketplace règles et vous en désabonner sur la AWS WAF console.

> **Important**
>
> Pour utiliser un groupe de AWS Marketplace règles dans une AWS Firewall Manager politique, chaque compte de votre organisation doit d'abord s'abonner à ce groupe de règles.

Pour s'abonner à un groupe de règles AWS Marketplace géré

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le panneau de navigation, sélectionnez AWS Marketplace.
3. Dans la section Produits du Marketplace disponibles, choisissez le nom d'un groupe de règles pour afficher les détails et les informations de tarification.
4. Pour vous abonner au groupe de règles, choisissez Continuer.

   > **Note**
   >
   > Si vous ne souhaitez pas vous abonner à ce groupe de règles, fermez simplement cette page dans votre navigateur.

5. Choisissez Configurer votre compte.

6. Ajoutez le groupe de règles à une liste ACL web, de la même manière que vous ajoutez une règle individuelle. Pour plus d'informations, consultez Création d'une liste ACL web ou Modification d'une ACL Web.

> **Note**
>
> Lorsque vous ajoutez un groupe de règles à une ACL Web, vous pouvez annuler les actions des règles du groupe de règles et du résultat du groupe de règles. Pour plus d'informations, consultez Options de dérogation aux actions pour les groupes de règles.

Une fois que vous êtes abonné à un groupe de AWS Marketplace règles, vous l'utilisez dans vos ACL Web comme dans les autres groupes de règles gérés. Pour plus d'informations, veuillez consulter Création d'une liste ACL web.

Se désabonner des groupes de règles AWS Marketplace gérés

Vous pouvez vous désabonner des groupes de AWS Marketplace règles sur la AWS WAF console.

> **Important**
>
> Pour arrêter les frais d'abonnement pour un groupe de règles AWS Marketplace géré, vous devez le supprimer de toutes les ACL Web incluses dans AWS WAF et dans toutes les AWS WAF politiques de Firewall Manager, en plus de vous désinscrire. Si vous vous désinscrivez d'un groupe de règles AWS Marketplace géré mais que vous ne le supprimez pas de vos ACL Web, l'abonnement continuera à vous être facturé.

Pour vous désabonner d'un groupe de règles AWS Marketplace géré

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Supprimez le groupe de règles de toutes les ACL web. Pour plus d'informations, consultez Modification d'une ACL Web.
3. Dans le panneau de navigation, sélectionnez AWS Marketplace.
4. Choisissez Manage your subscriptions.
5. Choisissez Annuler l'abonnement regard du nom du groupe de règles duquel vous souhaitez vous désabonner.

6. Choisissez Oui, annuler l'abonnement.

Groupes de AWS Marketplace règles de résolution des problèmes

Si vous constatez qu'un groupe de AWS Marketplace règles bloque le trafic légitime, vous pouvez résoudre le problème en effectuant les étapes suivantes.

Pour résoudre les problèmes d'un groupe de règles AWS Marketplace

1. Remplacez les actions pour qu'elles soient prises en compte dans les règles qui bloquent le trafic légitime. Vous pouvez identifier les règles bloquant des demandes spécifiques à l'aide des exemples AWS WAF de demandes ou AWS WAF des journaux. Vous pouvez identifier les règles en regardant le champ `ruleGroupId` dans le journal ou le champ `RuleWithinRuleGroup` dans la demande échantillonnée. Vous pouvez identifier la règle dans le modèle`<Seller Name>#<RuleGroup Name>#<Rule Name>`.
2. Si la définition de règles spécifiques pour ne compter que les demandes ne résout pas le problème, vous pouvez annuler toutes les actions des règles ou modifier l'action du groupe de AWS Marketplace règles lui-même de Aucune dérogation à Remplacer pour compter. La demande web peut ainsi passer, quelles que soient les actions des règles au sein du groupe de règles.
3. Après avoir annulé l'action de règle individuelle ou l'action de groupe de AWS Marketplace règles complète, contactez l'équipe d'assistance client du fournisseur du groupe de règles pour résoudre le problème plus en détail. Pour les coordonnées, consultez la liste du groupe de règles sur les pages de liste produit sur AWS Marketplace.

Contacter le AWS support

Pour tout problème AWS WAF lié à un groupe de règles géré par celui-ci AWS, contactez AWS Support. En cas de problème avec un groupe de règles géré par un AWS Marketplace vendeur, contactez l'équipe du support client du fournisseur. Pour trouver les informations de contact, consultez la liste du fournisseur sur AWS Marketplace.

Gestion de vos propres groupes de règles

Vous pouvez créer votre propre groupe de règles pour réutiliser des collections de règles que vous ne trouvez pas dans les offres de groupes de règles gérées ou que vous préférez gérer vous-même.

Les groupes de règles que vous créez contiennent des règles comme le fait une liste ACL web, et vous ajoutez des règles à un groupe de règles de la même manière que vous le faites pour une liste ACL web. Lorsque vous créez votre propre groupe de règles, vous devez définir une capacité maximale immuable pour celui-ci.

Rubriques

Création d'un groupe de règles

Pour créer un nouveau groupe de règles, suivez la procédure décrite sur cette page.

Pour créer un groupe de règles

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le panneau de navigation, choisissez Groupes de règles, puis Créer un groupe de règles.
3. Saisissez un nom et une description pour le groupe de règles. Vous les utiliserez pour identifier l'ensemble de règles permettant de le gérer et de l'utiliser.

   N'utilisez pas de noms commençant par `AWSShield`,`PreFM`, ou`PostFM`. Ces chaînes sont réservées ou peuvent prêter à confusion avec les groupes de règles gérés pour vous par d'autres services. veuillez consulter Groupes de règles fournis par d'autres services.

   > **Note**
   >
   > Vous ne pouvez pas modifier le nom une fois que vous créez la liste ACL web.

4. Pour Région, choisissez la région dans laquelle vous souhaitez stocker le groupe de règles. Pour utiliser un groupe de règles dans les ACL Web qui protègent les CloudFront distributions Amazon, vous devez utiliser le paramètre global. Vous pouvez également utiliser le paramètre global pour les applications régionales.
5. Choisissez Suivant.

6. Ajoutez des règles au groupe de règles à l'aide de l'Assistant Générateur de règles, comme vous le faites dans la gestion des listes ACL web. La seule différence est que vous ne pouvez pas ajouter un groupe de règles à un autre groupe de règles.
7. Pour Capacity (Capacité), définissez la valeur maximale pour le groupe de règles des unités de capacité ACL web (WCU). Paramètre immuable. Pour de plus amples informations sur les WCU, veuillez consulter AWS WAF unités de capacité ACL Web (WCU).

   Lorsque vous ajoutez des règles au groupe de règles, le panneau Ajouter des règles et définir la capacité affiche la capacité minimale requise, qui est basée sur les règles que vous avez déjà ajoutées. Vous pouvez l'utiliser ainsi que vos plans futurs pour le groupe de règles, et vous aider ainsi à estimer la capacité dont le groupe de règles aura besoin.
8. Vérifiez les paramètres du groupe de règles, puis choisissez Créer.

Modification d'un groupe de règles

Pour ajouter ou supprimer des règles dans un groupe de règles ou modifier les paramètres de configuration, accédez au groupe de règles en suivant la procédure décrite sur cette page.

> ⚠ Risque lié au trafic de production
>
> Si vous modifiez un groupe de règles que vous utilisez actuellement dans une ACL Web, ces modifications affecteront le comportement de votre ACL Web quel que soit l'endroit où il est utilisé. Assurez-vous de tester et d'ajuster toutes les modifications dans un environnement de test ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite vos règles mises à jour en mode décompte en fonction de votre trafic de production avant de les activer. Pour de plus amples informations, consultez Tester et ajuster vos AWS WAF protections.

Pour modifier un groupe de règles

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, sélectionnez Groupes de règles.
3. Choisissez le nom du groupe de règles que vous souhaitez modifier. La console vous amène à la page du groupe de règles.

4. Modifiez le groupe de règles selon vos besoins. Vous pouvez modifier les propriétés modifiables du groupe de règles, comme vous l'avez fait lors de sa création. La console enregistre vos modifications au fur et à mesure.

> **Note**
>
> Si vous modifiez le nom d'une règle et que vous souhaitez que le nom de la métrique de la règle reflète le changement, vous devez également mettre à jour le nom de la métrique. AWS WAF ne met pas automatiquement à jour le nom de la métrique d'une règle lorsque vous modifiez le nom de la règle. Vous pouvez modifier le nom de la métrique lorsque vous modifiez la règle dans la console, à l'aide de l'éditeur JSON de règles. Vous pouvez également modifier les deux noms via les API et dans toute liste JSON que vous utilisez pour définir votre ACL Web ou votre groupe de règles.

Incohérences temporaires lors des mises à jour

Lorsque vous créez ou modifiez une ACL Web ou d'autres AWS WAF ressources, les modifications mettent peu de temps à se propager à toutes les zones où les ressources sont stockées. Le temps de propagation peut aller de quelques secondes à plusieurs minutes.

Voici des exemples d'incohérences temporaires que vous pourriez remarquer lors de la propagation des modifications :

- Après avoir créé une ACL Web, si vous essayez de l'associer à une ressource, vous pouvez obtenir une exception indiquant que l'ACL Web n'est pas disponible.
- Une fois que vous avez ajouté un groupe de règles à une ACL Web, les nouvelles règles de groupe de règles peuvent être en vigueur dans une zone où l'ACL Web est utilisée et pas dans une autre.
- Une fois que vous avez modifié le paramètre d'une action de règle, vous pouvez voir l'ancienne action à certains endroits et la nouvelle action à d'autres.
- Après avoir ajouté une adresse IP à un ensemble d'adresses IP utilisé dans une règle de blocage, la nouvelle adresse peut être bloquée dans une zone alors qu'elle est toujours autorisée dans une autre.

Utilisation de votre groupe de règles dans une ACL Web

Pour utiliser un groupe de règles dans une ACL Web, vous l'ajoutez à l'ACL Web dans une déclaration de référence de groupe de règles.

> **Risque lié au trafic de production**
>
> Avant de déployer des modifications dans votre ACL Web pour le trafic de production, testez-les et ajustez-les dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite vos règles mises à jour en mode décompte avec votre trafic de production avant de les activer. Pour de plus amples informations, consultez Tester et ajuster vos AWS WAF protections.

> **Note**
>
> L'utilisation de plus de 1 500 WCU dans une ACL Web entraîne des coûts supérieurs au prix de base de l'ACL Web. Pour plus d'informations, veuillez consulter les sections AWS WAF unités de capacité ACL Web (WCU) et Tarification d'AWS WAF.

Sur la console, lorsque vous ajoutez ou mettez à jour les règles dans votre ACL Web, sur la page Ajouter des règles et des groupes de règles, choisissez Ajouter des règles, puis choisissez Ajouter mes propres règles et groupes de règles. Choisissez ensuite Groupe de règles et sélectionnez votre groupe de règles dans la liste.

Dans votre ACL Web, vous pouvez modifier le comportement d'un groupe de règles et ses règles en définissant les actions de règle individuelles sur Count ou toute autre action. Cela peut vous aider à tester un groupe de règles, à identifier les faux positifs à partir des règles d'un groupe de règles et à personnaliser la façon dont un groupe de règles géré traite vos demandes. Pour plus d’informations, consultez Options de dérogation aux actions pour les groupes de règles.

Si votre groupe de règles contient une instruction basée sur le taux, chaque ACL Web où vous utilisez le groupe de règles possède son propre suivi et sa propre gestion des taux pour la règle basée sur les taux, indépendamment de toute autre ACL Web dans laquelle vous utilisez le groupe de règles. Pour plus d’informations, consultez Instruction de règle basée sur un taux.

Incohérences temporaires lors des mises à jour

Lorsque vous créez ou modifiez une ACL Web ou d'autres AWS WAF ressources, les modifications mettent peu de temps à se propager à toutes les zones où les ressources sont stockées. Le temps de propagation peut aller de quelques secondes à plusieurs minutes.

Voici des exemples d'incohérences temporaires que vous pourriez remarquer lors de la propagation des modifications :

- Après avoir créé une ACL Web, si vous essayez de l'associer à une ressource, vous pouvez obtenir une exception indiquant que l'ACL Web n'est pas disponible.
- Une fois que vous avez ajouté un groupe de règles à une ACL Web, les nouvelles règles de groupe de règles peuvent être en vigueur dans une zone où l'ACL Web est utilisée et pas dans une autre.
- Une fois que vous avez modifié le paramètre d'une action de règle, vous pouvez voir l'ancienne action à certains endroits et la nouvelle action à d'autres.
- Après avoir ajouté une adresse IP à un ensemble d'adresses IP utilisé dans une règle de blocage, la nouvelle adresse peut être bloquée dans une zone alors qu'elle est toujours autorisée dans une autre.

Partage d'un groupe de règles avec un autre compte

Vous pouvez partager un groupe de règles avec d'autres comptes, afin qu'ils puissent l'utiliser. Vous pouvez partager avec un ou plusieurs comptes spécifiques, et vous pouvez partager avec tous les comptes d'une organisation.

Pour ce faire, vous utilisez l' AWS WAF API pour créer une politique pour le partage de groupes de règles que vous souhaitez. Pour plus d'informations, consultez PutPermissionPolicyla référence de AWS WAF l'API.

Suppression d'un groupe de règles

Suivez les instructions de cette section pour supprimer un groupe de règles.

Suppression d'ensembles et de groupes de règles référencés

Lorsque vous supprimez une entité que vous pouvez utiliser dans une ACL Web, telle qu'un ensemble d'adresses IP, un ensemble de modèles regex ou un groupe de règles, AWS WAF vérifie si l'entité est actuellement utilisée dans une ACL Web. S'il constate qu'il est en cours d'utilisation, il vous AWS WAF avertit. AWS WAF est presque toujours capable de déterminer si une entité est référencée par une ACL Web. Cependant, dans de rares cas, il peut ne pas être en mesure de le

faire. Si vous devez être sûr que rien n'utilise actuellement l'entité, vérifiez-la dans vos ACL Web avant de la supprimer. Si l'entité est un ensemble référencé, vérifiez également qu'aucun groupe de règles ne l'utilise.

Pour supprimer un groupe de règles

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, sélectionnez Groupes de règles.
3. Sélectionnez le groupe de règles que vous voulez supprimer et choisissez Supprimer.

Groupes de règles fournis par d'autres services

Si vous ou un administrateur de votre organisation utilisez AWS Firewall Manager ou gérez la protection des ressources AWS Shield Advanced à l'aide de cette méthode AWS WAF, des déclarations de référence à des groupes de règles peuvent être ajoutées aux ACL Web de votre compte.

Les noms de ces groupes de règles commencent par les chaînes suivantes :

- **`ShieldMitigationRuleGroup`**— Ces groupes de règles sont gérés AWS Shield Advanced et utilisés pour atténuer automatiquement les attaques DDoS de la couche application sur les ressources protégées de la couche application (couche 7).

  Lorsque vous activez l'atténuation automatique des attaques DDoS au niveau de la couche application pour une ressource protégée, Shield Advanced ajoute l'un de ces groupes de règles à l'ACL Web que vous avez associée à la ressource. Shield Advanced attribue à l'instruction de référence du groupe de règles un paramètre de priorité de 10 000 000, afin qu'elle s'exécute conformément aux règles que vous avez configurées dans l'ACL Web. Pour plus d'informations sur ces groupes de règles, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

  > **Warning**
  >
  > N'essayez pas de gérer manuellement ce groupe de règles dans votre ACL Web. En particulier, ne supprimez pas manuellement l'instruction de référence du groupe de `ShieldMitigationRuleGroup` règles de votre ACL Web. Cela pourrait avoir des conséquences imprévues sur toutes les ressources associées à l'ACL Web. Utilisez plutôt

Shield Advanced pour désactiver l'atténuation automatique pour les ressources associées à l'ACL Web. Shield Advanced supprimera le groupe de règles pour vous lorsqu'il n'est pas nécessaire pour une atténuation automatique.

- **`PREFMManaged`et `POSTFMManaged`** — Ces groupes de règles sont gérés par AWS Firewall Manager. Firewall Manager les fournit au sein de listes de contrôle d'accès Web créées et gérées par Firewall Manager. Les noms des ACL Web commencent `FMManagedWebACLV2` par. Pour plus d'informations sur ces ACL Web et ces groupes de règles, consultezAWS WAF politiques.

AWS WAF règles

Une AWS WAF règle définit comment inspecter les requêtes Web HTTP (S) et les mesures à prendre pour traiter une demande lorsqu'elle répond aux critères d'inspection. Vous définissez des règles uniquement dans le contexte d'un groupe de règles ou d'une ACL Web.

Les règles n'existent pas AWS WAF en elles-mêmes. Ce ne sont pas AWS des ressources et ils n'ont pas de noms de ressources Amazon (ARN). Vous pouvez accéder à une règle par son nom dans le groupe de règles ou l'ACL web où elle est définie. Vous pouvez gérer les règles et les copier vers d'autres ACL Web à l'aide de la vue JSON du groupe de règles ou de l'ACL Web qui contient la règle. Vous pouvez également les gérer via le générateur de règles de AWS WAF console, disponible pour les ACL Web et les groupes de règles.

Nom de la règle

Chaque règle nécessite un nom. Évitez les noms commençant par `AWS` et ceux utilisés pour les groupes de règles ou les règles gérées pour vous par d'autres services. veuillez consulter Groupes de règles fournis par d'autres services.

> **Note**
>
> Si vous modifiez le nom d'une règle et que vous souhaitez que le nom de la métrique de la règle reflète le changement, vous devez également mettre à jour le nom de la métrique. AWS WAF ne met pas automatiquement à jour le nom de la métrique d'une règle lorsque vous modifiez le nom de la règle. Vous pouvez modifier le nom de la métrique lorsque vous modifiez la règle dans la console, à l'aide de l'éditeur JSON de règles. Vous pouvez également modifier les deux noms via les API et dans toute liste JSON que vous utilisez pour définir votre ACL Web ou votre groupe de règles.

Déclaration de règle

Chaque règle nécessite également une déclaration de règle qui définit la manière dont la règle inspecte les requêtes Web. L'instruction de règle peut contenir d'autres instructions imbriquées à n'importe quelle profondeur, en fonction de la règle et du type d'instruction. Certains énoncés de règles utilisent des ensembles de critères. Par exemple, vous pouvez spécifier jusqu'à 10 000 adresses IP ou plages d'adresses IP pour une règle de correspondance des ensembles d'adresses IP.

Vous pouvez définir des règles qui vérifient les critères suivants :

- Les scripts qui sont susceptibles d'être malveillants. Les pirates intègrent des scripts qui peuvent exploiter les vulnérabilités des applications web. Il s'agit de scripts inter-sites.
- Les adresses IP ou les plages d'adresses IP d'où proviennent les requêtes.
- Pays ou emplacement géographique d'où proviennent les demandes.
- Longueur d'une partie spécifiée de la demande, telle que la chaîne de requête.
- Le code SQL susceptible d'être malveillants. Les pirates essaient d'extraire les données de votre base de données en intégrant un code SQL malveillant dans une requête web. Cette opération s'appelle injection SQL.
- Les chaînes qui apparaissent dans la requête, par exemple, les valeurs qui apparaissent dans l'en-tête `User-Agent` ou les chaînes de texte qui apparaissent dans la chaîne de requête. Vous pouvez également utiliser des expressions régulières (regex) pour spécifier ces chaînes.
- Étiquettes que les règles précédentes de l'ACL Web ont ajoutées à la demande.

Outre les instructions comportant des critères d'inspection des requêtes Web, comme ceux de la liste précédente, prennent AWS WAF en charge les instructions logiques pour `AND`, `OR`, et `NOT` que vous pouvez utiliser pour combiner des instructions dans une règle.

Par exemple, sur la base des demandes récentes que vous avez reçues d'un attaquant, vous pouvez créer une règle avec une `AND` instruction logique qui combine les instructions imbriquées suivantes :

- Les requêtes proviennent de 192.0.2.44.
- Elles contiennent la valeur `BadBot` dans l'en-tête `User-Agent`.
- Elles semblent inclure du code de type SQL dans la chaîne de requête.

Dans ce cas, la requête Web doit correspondre à toutes les instructions pour obtenir une correspondance pour le niveau supérieur`AND`.

Rubriques

Action de la règle

L'action de règle indique AWS WAF ce qu'il faut faire avec une requête Web lorsqu'elle répond aux critères définis dans la règle. Vous pouvez éventuellement ajouter un comportement personnalisé à chaque action de règle.

> **Note**
>
> Les actions relatives aux règles peuvent être terminales ou non. Une action de terminaison arrête l'évaluation ACL Web de la demande et la laisse continuer vers votre application protégée ou la bloque.

Voici les options d'action de la règle :

- Allow— AWS WAF permet à la demande d'être transmise à la AWS ressource protégée pour traitement et réponse. Il s'agit d'une action terminale. Dans les règles que vous définissez, vous pouvez insérer des en-têtes personnalisés dans la demande avant de la transmettre à la ressource protégée.
- Block— AWS WAF bloque la demande. Il s'agit d'une action terminale. Par défaut, votre AWS ressource protégée répond par un code d'`403 (Forbidden)`état HTTP. Dans les règles que vous définissez, vous pouvez personnaliser la réponse. En cas de AWS WAF blocage d'une demande, les paramètres Block d'action déterminent la réponse que la ressource protégée renvoie au client.
- Count— AWS WAF compte la demande mais ne détermine pas s'il faut l'autoriser ou la bloquer. Il s'agit d'une action sans fin. AWS WAF continue de traiter les règles restantes dans l'ACL Web.

Dans les règles que vous définissez, vous pouvez insérer des en-têtes personnalisés dans la demande et ajouter des libellés auxquels d'autres règles peuvent correspondre.

- CAPTCHAet Challenge — AWS WAF utilise des puzzles CAPTCHA et des défis silencieux pour vérifier que la demande ne provient pas d'un bot, et AWS WAF utilise des jetons pour suivre les récentes réponses positives des clients.

  Les puzzles CAPTCHA et les défis silencieux ne peuvent être exécutés que lorsque les navigateurs accèdent à des points de terminaison HTTPS. Les clients du navigateur doivent fonctionner dans des contextes sécurisés pour acquérir des jetons.

  > **Note**
  >
  > Des frais supplémentaires vous sont facturés lorsque vous utilisez l'action CAPTCHA ou la Challenge règle dans l'une de vos règles ou en tant que dérogation d'action de règle dans un groupe de règles. Pour plus d'informations, consultez Tarification d'AWS WAF.

  Ces actions de règles peuvent être terminales ou non, selon l'état du jeton dans la demande :

  - Non résiliable pour un jeton valide et non expiré : si le jeton est valide et non expiré conformément au CAPTCHA configuré ou à la durée d'immunité au défi, AWS WAF gère la demande de la même manière que l'action. Count AWS WAF continue d'inspecter la requête Web en fonction des règles restantes de l'ACL Web. Comme pour la Count configuration, dans les règles que vous définissez, vous pouvez éventuellement configurer ces actions avec des en-têtes personnalisés à insérer dans la demande, et vous pouvez ajouter des étiquettes auxquelles d'autres règles peuvent correspondre.
  - Terminer par une demande bloquée pour un jeton non valide ou expiré — Si le jeton n'est pas valide ou si l'horodatage indiqué est expiré, AWS WAF met fin à l'inspection de la requête Web et bloque la demande, comme dans le cas de l'action. Block AWS WAF répond ensuite au client avec un code de réponse personnalisé. En CAPTCHA effet, si le contenu de la demande indique que le navigateur client peut la gérer, AWS WAF envoie un casse-tête CAPTCHA dans un JavaScript interstitiel, conçu pour distinguer les clients humains des robots. Pour l'Challengeaction, AWS WAF envoie un JavaScript interstitiel avec un défi silencieux conçu pour distinguer les navigateurs normaux des sessions exécutées par des robots.

  Pour plus d'informations, consultez CAPTCHAet Challenge dans AWS WAF.

Pour plus d'informations sur la personnalisation des demandes et des réponses, consultezDemandes et réponses Web personnalisées dans AWS WAF.

Pour plus d'informations sur l'ajout d'étiquettes aux demandes correspondantes, consultezAWS WAF étiquettes sur les requêtes Web.

Pour plus d'informations sur la façon dont l'ACL Web et les paramètres des règles interagissent, consultezÉvaluation des règles ACL Web et des groupes de règles.

Notions de base sur les énoncés

Les instructions de règle font partie d'une règle qui indique AWS WAF comment inspecter une requête Web. Lorsque AWS WAF les critères d'inspection sont trouvés dans une requête Web, nous disons que la requête Web correspond à la déclaration. Chaque instruction de règle spécifie ce qu'il faut rechercher et comment, selon le type d'instruction.

Chaque règle AWS WAF contient une seule instruction de règle de niveau supérieur, qui peut contenir d'autres instructions. Les déclarations de règle peuvent être très simples. Par exemple, vous pouvez avoir une instruction qui fournit un ensemble de pays d'origine pour lesquels inspecter vos requêtes Web ou vous pouvez avoir une déclaration de règle dans une ACL Web qui fait simplement référence à un groupe de règles. Les instructions de règle peuvent également être très complexes. Par exemple, vous pouvez avoir une instruction qui combine de nombreuses autres instructions avec AND des OR NOT instructions logiques et.

Pour la plupart des règles, vous pouvez ajouter un AWS WAF étiquetage personnalisé aux demandes correspondantes. Les règles des groupes de règles AWS gérées ajoutent des étiquettes aux demandes correspondantes. Les étiquettes ajoutées par une règle fournissent des informations sur la demande aux règles qui sont évaluées ultérieurement dans l'ACL Web, ainsi que dans AWS WAF les journaux et les métriques. Pour plus d'informations sur l'étiquetage, reportez-vous AWS WAF étiquettes sur les requêtes Web aux sections etDéclaration relative à la règle de correspondance des étiquettes.

Instructions de règles d'imbrication

AWS WAF prend en charge l'imbrication pour de nombreuses instructions de règles, mais pas pour toutes. Par exemple, vous ne pouvez pas imbriquer une instruction de groupe de règles dans une autre instruction. Vous devez utiliser l'imbrication pour certains scénarios, tels que les instructions scope-down et les instructions logiques. Les instructions de règles et les détails des règles qui suivent décrivent les capacités d'imbrication et les exigences pour chaque catégorie et règle.

L'éditeur visuel des règles de la console ne prend en charge qu'un seul niveau d'imbrication pour les instructions de règles. Par exemple, vous pouvez imbriquer de nombreux types d'instructions dans une logique AND ou une OR règle, mais vous ne pouvez pas en imbriquer une autreAND, car cela nécessite un deuxième niveau d'imbrication. OR Pour implémenter plusieurs niveaux d'imbrication, fournissez la définition de la règle au format JSON, soit via l'éditeur de règles JSON de la console, soit via les API.

Rubriques

- Spécification et gestion des composants de requête Web
- Déclarations de portée réduite
- Instructions faisant référence à un ensemble ou à un groupe de règles

Spécification et gestion des composants de requête Web

Cette section décrit les paramètres que vous pouvez spécifier dans les instructions de règle qui inspectent un composant de la requête Web. Pour plus d'informations sur l'utilisation, consultez les instructions de règles individuelles à l'adresseFaire correspondre les déclarations des règles.

Un sous-ensemble de ces composants de requête Web peut également être utilisé dans des règles basées sur le taux, sous forme de clés d'agrégation de demandes personnalisées. Pour plus d'informations, veuillez consulter Options et clés d'agrégation de règles basées sur le taux.

Pour les paramètres du composant de demande, vous spécifiez le type de composant lui-même, ainsi que toutes les options supplémentaires, en fonction du type de composant. Par exemple, lorsque vous inspectez un type de composant contenant du texte, vous pouvez lui appliquer des transformations de texte avant de l'inspecter.

> **Note**
>
> Sauf indication contraire, si une requête Web ne possède pas le composant de demande spécifié dans l'instruction de règle, la demande est AWS WAF évaluée comme ne correspondant pas aux critères de la règle.

Table des matières

  - En-tête seul
  - Tous les en-têtes
  - Ordre des en-têtes
  - Cookies
  - chemin de l'URI
  - Empreinte digitale JA3
  - Chaîne de requête
  - Paramètre de requête unique
  - Tous les paramètres de requête
  - Corps de texte
  - corps JSON
- Adresse IP transférée
- Options pour inspecter les pseudo-en-têtes HTTP/2
- Options de transformation du texte

Options de composants de demande

Cette section décrit les composants de la requête Web que vous pouvez spécifier pour inspection. Vous spécifiez le composant de demande pour les instructions de règle de correspondance qui recherchent des modèles dans la requête Web. Ces types d'instructions incluent les instructions de correspondance de chaîne, de correspondance régulière, de contrainte de taille et d'attaque par injection SQL. Pour plus d'informations sur l'utilisation de ces paramètres de composant de requête, consultez les instructions de règle individuelles à l'adresse Faire correspondre les déclarations des règles

Sauf indication contraire, si une requête Web ne possède pas le composant de demande spécifié dans l'instruction de règle, la demande est AWS WAF évaluée comme ne correspondant pas aux critères de la règle.

> **Note**
>
> Vous spécifiez un composant de demande unique pour chaque instruction de règle qui le requiert. Pour inspecter plusieurs composants d'une demande, créez une instruction de règle pour chacun d'eux.

La documentation de la AWS WAF console et de l'API fournit des conseils sur les paramètres des composants de demande aux emplacements suivants :

- Générateur de règles sur la console : dans les paramètres de déclaration pour un type de règle normal, choisissez le composant que vous souhaitez inspecter dans la boîte de dialogue Inspecter sous Composants de demande.
- Contenu de la déclaration d'API — `FieldToMatch`

Le reste de cette section décrit les options relatives à la partie de la requête Web à inspecter.

Rubriques

Méthode HTTP

Inspecte la méthode HTTP pour la demande. La méthode HTTP indique le type d'opération que la requête Web demande à votre ressource protégée d'effectuer, telle que `POST` ou`GET`.

En-tête seul

Inspecte un seul en-tête nommé dans la demande.

Pour cette option, vous spécifiez le nom de l'en-tête, par exemple, `User-Agent` ou`Referer`. La chaîne correspondant au nom ne distingue pas les majuscules et minuscules.

Tous les en-têtes

Inspecte tous les en-têtes de demande, y compris les cookies. Vous pouvez appliquer un filtre pour inspecter un sous-ensemble de tous les en-têtes.

Pour cette option, vous devez fournir les spécifications suivantes :

- Modèles de correspondance : filtre à utiliser pour obtenir un sous-ensemble d'en-têtes à inspecter. AWS WAF recherche ces modèles dans les touches d'en-tête.

  Le paramètre des modèles de correspondance peut être l'un des suivants :

  - Toutes — Faites correspondre toutes les clés. Évaluez les critères d'inspection des règles pour tous les en-têtes.
  - En-têtes exclus : inspectez uniquement les en-têtes dont les clés ne correspondent à aucune des chaînes que vous spécifiez ici. La correspondance de chaîne pour une clé ne fait pas la distinction majuscules/minuscules.
  - En-têtes inclus : inspectez uniquement les en-têtes dont la clé correspond à l'une des chaînes que vous spécifiez ici. La correspondance de chaîne pour une clé ne fait pas la distinction majuscules/minuscules.
- Champ d'application du match : parties des en-têtes qui AWS WAF doivent être inspectées selon les critères d'inspection des règles. Vous pouvez spécifier des clés, des valeurs ou tout pour inspecter à la fois les clés et les valeurs pour détecter une correspondance.

  Tout ne nécessite pas qu'une correspondance soit trouvée dans les clés et qu'une correspondance soit trouvée dans les valeurs. Cela nécessite qu'une correspondance soit trouvée dans les clés ou les valeurs, ou dans les deux. Pour exiger une correspondance entre les clés et les valeurs, utilisez une AND instruction logique pour combiner deux règles de correspondance, l'une inspectant les clés et l'autre les valeurs.
- Gestion des données surdimensionnées — AWS WAF Comment gérer les demandes dont les données d'en-tête sont supérieures à ce que AWS WAF vous pouvez inspecter ? AWS WAF peut inspecter au maximum les 8 premiers Ko (8 192 octets) des en-têtes de requête et au plus les 200 premiers en-têtes. Le contenu peut être consulté AWS WAF jusqu'à la première limite atteinte. Vous pouvez choisir de poursuivre l'inspection ou de sauter l'inspection et de marquer la demande comme correspondant ou non à la règle. Pour plus d'informations sur la gestion du contenu surdimensionné, consultezGestion des composants de demande surdimensionnés dans AWS WAF.

Ordre des en-têtes

Inspectez une chaîne contenant la liste des noms d'en-tête de la demande, classés tels qu'ils apparaissent dans la demande Web qui est AWS WAF reçue pour inspection. AWS WAF génère la chaîne, puis l'utilise comme champ pour faire correspondre le composant lors de son inspection. AWS WAF sépare les noms des en-têtes dans la chaîne par des deux-points et sans espaces ajoutés, par exemple`host:user-agent:accept:authorization:referer`.

Pour cette option, vous devez fournir les spécifications suivantes :

- Gestion des données surdimensionnées — Comment AWS WAF gérer les demandes dont les données d'en-tête sont plus nombreuses ou plus volumineuses que celles que l' AWS WAF on peut inspecter ? AWS WAF peut inspecter au maximum les 8 premiers Ko (8 192 octets) des en-têtes de requête et au plus les 200 premiers en-têtes. Le contenu peut être consulté AWS WAF jusqu'à la première limite atteinte. Vous pouvez choisir de continuer à inspecter les en-têtes disponibles ou d'ignorer l'inspection et de marquer la demande comme correspondant ou non à la règle. Pour plus d'informations sur la gestion du contenu surdimensionné, consultezGestion des composants de demande surdimensionnés dans AWS WAF.

Cookies

Inspecte tous les cookies de demande. Vous pouvez appliquer un filtre pour inspecter un sous-ensemble de tous les cookies.

Pour cette option, vous devez fournir les spécifications suivantes :

- Modèles de correspondance : filtre à utiliser pour obtenir un sous-ensemble de cookies à inspecter. AWS WAF recherche ces modèles dans les clés des cookies.

  Le paramètre des modèles de correspondance peut être l'un des suivants :

  - Toutes — Faites correspondre toutes les clés. Évaluez les critères d'inspection des règles pour tous les cookies.
  - Cookies exclus : inspectez uniquement les cookies dont les clés ne correspondent à aucune des chaînes que vous spécifiez ici. La correspondance de chaîne pour une clé distingue les majuscules et minuscules et doit être exacte.
  - Cookies inclus : inspectez uniquement les cookies dont la clé correspond à l'une des chaînes que vous spécifiez ici. La correspondance de chaîne pour une clé distingue les majuscules et minuscules et doit être exacte.

- Champ d'application du match : parties des cookies qui AWS WAF doivent être inspectées selon les critères d'inspection des règles. Vous pouvez spécifier des clés, des valeurs ou tout pour les clés et les valeurs.

  Tout ne nécessite pas qu'une correspondance soit trouvée dans les clés et qu'une correspondance soit trouvée dans les valeurs. Cela nécessite qu'une correspondance soit trouvée dans les clés ou les valeurs, ou dans les deux. Pour exiger une correspondance entre les clés et les valeurs, utilisez une AND instruction logique pour combiner deux règles de correspondance, l'une inspectant les clés et l'autre les valeurs.
- Gestion des données surdimensionnées — Comment AWS WAF gérer les demandes contenant des données de cookies d'une taille supérieure à ce que AWS WAF vous pouvez inspecter ? AWS WAF peut inspecter au maximum les 8 premiers Ko (8 192 octets) des cookies de demande et au plus les 200 premiers cookies. Le contenu peut être consulté AWS WAF jusqu'à la première limite atteinte. Vous pouvez choisir de poursuivre l'inspection ou de sauter l'inspection et de marquer la demande comme correspondant ou non à la règle. Pour plus d'informations sur la gestion du contenu surdimensionné, consultezGestion des composants de demande surdimensionnés dans AWS WAF.

chemin de l'URI

Inspecte la partie d'une URL qui identifie une ressource, par exemple,`/images/daily-ad.jpg`. Pour plus d'informations, voir Uniform Resource Identifier (URI) : syntaxe générique.

Si vous n'utilisez pas de transformation de texte avec cette option, elle AWS WAF ne normalise pas l'URI et ne l'inspecte pas exactement telle qu'elle est reçue du client dans la demande. Pour plus d'informations sur les transformations de texte, consultezOptions de transformation du texte.

Empreinte digitale JA3

Inspecte l'empreinte JA3 de la demande.

> **Note**
>
> L'inspection des empreintes digitales JA3 n'est disponible que pour les CloudFront distributions Amazon et les équilibreurs de charge d'application.

L'empreinte JA3 est un hachage de 32 caractères dérivé du client TLS Hello d'une demande entrante. Cette empreinte sert d'identifiant unique pour la configuration TLS du client. AWS WAF

calcule et enregistre cette empreinte pour chaque demande contenant suffisamment d'informations TLS Client Hello pour le calcul. Presque toutes les demandes sur le Web incluent ces informations.

Comment obtenir l'empreinte JA3 d'un client

Vous pouvez obtenir l'empreinte JA3 pour les demandes d'un client à partir des journaux ACL Web. S'il AWS WAF est capable de calculer l'empreinte digitale, il l'inclut dans les journaux. Pour plus d'informations sur les champs de journalisation, consultezChamps de journal.

Exigences relatives à l'énoncé des règles

Vous pouvez inspecter l'empreinte JA3 uniquement dans une instruction de correspondance de chaîne définie pour correspondre exactement à la chaîne que vous fournissez. Fournissez la chaîne d'empreinte JA3 issue des journaux dans votre spécification d'instruction de correspondance de chaîne, afin qu'elle corresponde à toute future demande ayant la même configuration TLS. Pour plus d'informations sur l'instruction de correspondance des chaînes, consultezInstruction de correspondance de chaîne de règle.

Vous devez fournir un comportement de remplacement pour cette déclaration de règle. Le comportement de remplacement est le statut de correspondance que vous souhaitez attribuer AWS WAF à la requête Web si AWS WAF vous ne parvenez pas à calculer l'empreinte JA3. Si vous choisissez de faire correspondre, AWS WAF traite la demande comme correspondant à l'instruction de règle et applique l'action de règle à la demande. Si vous choisissez de ne pas correspondre, AWS WAF traite la demande comme ne correspondant pas à l'instruction de règle.

Pour utiliser cette option de correspondance, vous devez enregistrer votre trafic ACL Web. Pour plus d'informations, veuillez consulter Journalisation AWS WAF du trafic ACL Web.

Chaîne de requête

Inspecte la partie de l'URL qui apparaît après un ? caractère, le cas échéant.

> **Note**
>
> Pour les instructions de correspondance basées sur des scripts intersites, nous vous recommandons de choisir Tous les paramètres de requête au lieu de Chaîne de requête. Le choix de tous les paramètres de requête ajoute 10 WCU au coût de base.

Paramètre de requête unique

Inspecte un seul paramètre de requête que vous avez défini dans le cadre de la chaîne de requête. AWS WAF inspecte la valeur du paramètre que vous spécifiez.

Pour cette option, vous devez également spécifier un argument de requête. Par exemple, si l'URL est`www.xyz.com?UserName=abc&SalesRegion=seattle`, vous pouvez spécifier `UserName` ou `SalesRegion` pour l'argument de requête. La longueur maximale du nom de l'argument est de 30 caractères. Le nom ne distingue pas les majuscules et minuscules. Ainsi, si vous le spécifiez`UserName`, il AWS WAF correspond à toutes les variantes de`UserName`, y compris `username` et`UsERName`.

Si la chaîne de requête contient plusieurs instances de l'argument de requête que vous avez spécifié, AWS WAF examine toutes les valeurs pour détecter une correspondance, en utilisant la OR logique. Par exemple, dans l'URL `www.xyz.com?SalesRegion=boston&SalesRegion=seattle`, AWS WAF évalue le nom que vous avez spécifié par rapport à `boston` et `seattle`. Si l'un ou l'autre est une correspondance, l'inspection est une correspondance.

Tous les paramètres de requête

Inspecte tous les paramètres de requête contenus dans la demande. Cela est similaire au choix d'un composant de requête unique, mais AWS WAF inspecte les valeurs de tous les arguments de la chaîne de requête. Par exemple, si l'URL est `www.xyz.com?UserName=abc&SalesRegion=seattle`, AWS WAF déclenche une correspondance si la valeur de `UserName` ou `SalesRegion` correspond aux critères d'inspection.

Le choix de cette option ajoute 10 WCU au coût de base.

Corps de texte

Inspecte le corps de la demande, évalué sous forme de texte brut. Vous pouvez également évaluer le corps au format JSON à l'aide du type de JSON contenu.

Le corps de la demande est la partie de la demande qui suit immédiatement les en-têtes de la demande. Il contient toutes les données supplémentaires nécessaires à la requête Web, par exemple les données d'un formulaire.

- Dans la console, sélectionnez cette option dans le corps de l'option de demande, en sélectionnant le type de contenu Texte brut.
- Dans l'API, dans la `FieldToMatch` spécification de la règle, vous spécifiez `Body` d'inspecter le corps de la demande sous forme de texte brut.

Pour Application Load Balancer et AWS AppSync, AWS WAF peut inspecter les 8 premiers Ko du corps d'une requête. Par défaut CloudFront, API Gateway, Amazon Cognito, App Runner et Verified Access AWS WAF peuvent inspecter les 16 premiers Ko, et vous pouvez augmenter la limite jusqu'à 64 Ko dans votre configuration ACL Web. Pour plus d'informations, consultez Gestion des limites de taille des organismes inspectés.

Vous devez spécifier la gestion des surdimensionnements pour ce type de composant. La gestion des données surdimensionnées définit le AWS WAF mode de traitement des demandes dont les données corporelles sont trop volumineuses pour AWS WAF être inspectées. Vous pouvez choisir de poursuivre l'inspection ou de sauter l'inspection et de marquer la demande comme correspondant ou non à la règle. Pour plus d'informations sur la gestion du contenu surdimensionné, consultezGestion des composants de demande surdimensionnés dans AWS WAF.

Vous pouvez également évaluer le corps sous forme de JSON analysé. Pour plus d'informations à ce sujet, consultez la section qui suit.

corps JSON

Inspecte le corps de la demande, évalué au format JSON. Vous pouvez également évaluer le corps sous forme de texte brut.

Le corps de la demande est la partie de la demande qui suit immédiatement les en-têtes de la demande. Il contient toutes les données supplémentaires nécessaires à la requête Web, par exemple les données d'un formulaire.

- Dans la console, vous pouvez le sélectionner dans le choix de l'option de demande Body, en sélectionnant le choix du type de contenu JSON.
- Dans l'API, dans la `FieldToMatch` spécification de la règle, vous spécifiez`JsonBody`.

Pour Application Load Balancer et AWS AppSync, AWS WAF peut inspecter les 8 premiers Ko du corps d'une requête. Par défaut CloudFront, API Gateway, Amazon Cognito, App Runner et Verified Access AWS WAF peuvent inspecter les 16 premiers Ko, et vous pouvez augmenter la limite jusqu'à 64 Ko dans votre configuration ACL Web. Pour plus d'informations, consultez Gestion des limites de taille des organismes inspectés.

Vous devez spécifier la gestion des surdimensionnements pour ce type de composant. La gestion des données surdimensionnées définit le AWS WAF mode de traitement des demandes dont les données corporelles sont trop volumineuses pour AWS WAF être inspectées. Vous pouvez choisir de

poursuivre l'inspection ou de sauter l'inspection et de marquer la demande comme correspondant ou non à la règle. Pour plus d'informations sur la gestion du contenu surdimensionné, consultezGestion des composants de demande surdimensionnés dans AWS WAF.

Le choix de cette option double le coût de base des WCU du relevé de match. Par exemple, si le coût de base de l'instruction match est de 5 WCU sans analyse JSON, l'utilisation de l'analyse JSON double le coût à 10 WCU.

Étapes et options pour l'inspection du corps au format JSON

Lorsqu'il AWS WAF inspecte le corps de la requête Web au format JSON, il exécute des étapes pour analyser le corps et extraire les éléments JSON à des fins d'inspection. Vous trouverez ci-dessous la liste des étapes et des options de configuration supplémentaires pour ce type de composant de demande.

1. Analyse le contenu du corps : AWS WAF analyse le contenu du corps de la requête Web afin d'extraire les éléments JSON à des fins d'inspection. AWS WAF fait de son mieux pour analyser l'intégralité du contenu du corps, mais l'analyse peut échouer en raison de divers états d'erreur dans le contenu. Les exemples incluent les caractères non valides, les clés dupliquées, la troncature et le contenu dont le nœud racine n'est ni un objet ni un tableau.

   L'option Body parsing fallback behavior détermine ce qui se passe si elle AWS WAF ne parvient pas à analyser complètement le corps JSON :

   - Aucun (comportement par défaut) : AWS WAF évalue le contenu uniquement jusqu'au point où il a rencontré une erreur d'analyse.
   - Evaluer en tant que chaîne - Inspectez le corps en tant que texte brut. AWS WAF applique les transformations de texte et les critères d'inspection que vous avez définis pour l'inspection JSON à la chaîne du corps du texte.
   - Match : traitez la requête Web comme correspondant à l'instruction de règle. AWS WAF applique l'action de règle à la demande.
   - Aucune correspondance : considérez la requête Web comme ne correspondant pas à l'instruction de règle.

   > **Note**
   >
   > Ce comportement de secours ne se déclenche qu'en cas d' AWS WAF erreur lors de l'analyse de la chaîne JSON.

L'analyse ne valide pas complètement le JSON

AWS WAF l'analyse ne valide pas complètement la chaîne JSON d'entrée, de sorte que l'analyse peut réussir même pour un JSON non valide.

Par exemple, AWS WAF analyse le code JSON non valide suivant sans erreur :

- Virgule manquante : `{"key1":"value1""key2":"value2"}`
- Deux-points manquant : `{"key1":"value1","key2""value2"}`
- Deux-points supplémentaire : `{"key1"::"value1","key2""value2"}`

Dans de tels cas où l'analyse réussit mais où le résultat n'est pas un JSON complètement valide, le résultat des étapes suivantes de l'évaluation peut varier. L'extraction peut omettre certains éléments ou l'évaluation des règles peut avoir des résultats inattendus. Nous vous recommandons de valider le JSON que vous recevez dans votre application et de traiter le JSON non valide selon les besoins.

2. Extraire les éléments JSON : AWS WAF identifie le sous-ensemble d'éléments JSON à inspecter en fonction de vos paramètres :
   - L'option JSON match scope indique les types d'éléments du JSON qui AWS WAF doivent être inspectés.

     Vous pouvez spécifier des clés, des valeurs ou tout pour les clés et les valeurs.

     Tout ne nécessite pas qu'une correspondance soit trouvée dans les clés et qu'une correspondance soit trouvée dans les valeurs. Cela nécessite qu'une correspondance soit trouvée dans les clés ou les valeurs, ou dans les deux. Pour exiger une correspondance entre les clés et les valeurs, utilisez une `AND` instruction logique pour combiner deux règles de correspondance, l'une inspectant les clés et l'autre les valeurs.
   - L'option Contenu à inspecter indique comment filtrer l'ensemble d'éléments en fonction du sous-ensemble que vous AWS WAF souhaitez inspecter.

     Vous devez spécifier l'une des options suivantes :
     - Contenu JSON complet : évaluez tous les éléments.
     - Éléments inclus uniquement : évaluez uniquement les éléments dont les chemins correspondent aux critères de pointeur JSON que vous fournissez. N'utilisez pas cette option pour indiquer tous les chemins dans le JSON. Utilisez plutôt le contenu JSON complet.

Pour plus d'informations sur la syntaxe du pointeur JSON, consultez la documentation du pointeur JSON (JavaScript Object Notation) de l'Internet Engineering Task Force (IETF).

Par exemple, dans la console, vous pouvez fournir les informations suivantes :

```
/dogs/0/name
/dogs/1/name
```

Dans l'API ou la CLI, vous pouvez fournir les éléments suivants :

```
"IncludedPaths": ["/dogs/0/name", "/dogs/1/name"]
```

Supposons, par exemple, que le paramètre Contenu à inspecter soit Uniquement les éléments inclus et que le paramètre Éléments inclus soit défini comme tel/a/b.

Pour l'exemple de corps JSON suivant :

```
{
  "a":{
    "c":"d",
    "b":{
      "e":{
        "f":"g"
      }
    }
  }
}
```

Les ensembles d'éléments qui AWS WAF vérifieraient chaque paramètre de portée de correspondance JSON sont répertoriés ci-dessous. Notez que la cléb, qui fait partie du chemin des éléments inclus, n'est pas évaluée.

- Tous :e, f, etg.
- Clés : e etf.
- Valeurs :g.

3. Inspectez le jeu d'éléments JSON : AWS WAF applique les transformations de texte que vous avez spécifiées aux éléments JSON extraits, puis compare l'ensemble d'éléments obtenu aux critères de correspondance de l'instruction de règle. Il s'agit du même comportement de

transformation et d'évaluation que pour les autres composants de requête Web. Si l'un des éléments JSON extraits correspond, la requête Web correspond à la règle.

Adresse IP transférée

Cette section s'applique aux instructions de règles qui utilisent l'adresse IP d'une requête Web. Par défaut, AWS WAF utilise l'adresse IP de l'origine de la requête Web. Toutefois, si une requête Web passe par un ou plusieurs proxys ou équilibreurs de charge, l'origine de la demande Web contiendra l'adresse du dernier proxy, et non l'adresse d'origine du client. Dans ce cas, l'adresse du client d'origine est généralement transmise dans un autre en-tête HTTP. Cet en-tête est généralement `X-Forwarded-For` (XFF), mais il peut être différent.

Déclarations de règles utilisant des adresses IP

Les instructions de règle qui utilisent les adresses IP sont les suivantes :

- Correspondance d'ensemble d'adresses IP- Vérifie si l'adresse IP correspond aux adresses définies dans un ensemble d'adresses IP.
- Correspondance géographique- Utilise l'adresse IP pour déterminer le pays et la région d'origine et compare le pays d'origine à une liste de pays.
- Instruction de règle basée sur un taux- Peut agréger les demandes par adresse IP pour s'assurer qu'aucune adresse IP individuelle n'envoie de demandes à un rythme trop élevé. Vous pouvez utiliser l'agrégation d'adresses IP seule ou en combinaison avec d'autres clés d'agrégation.

Vous pouvez demander d' AWS WAF utiliser une adresse IP transférée pour chacune de ces instructions de règle, que ce soit à partir de l'`X-Forwarded-For`en-tête ou d'un autre en-tête HTTP, au lieu d'utiliser l'origine de la requête Web. Pour plus de détails sur la manière de fournir les spécifications, consultez les instructions relatives aux différents types d'instructions de règles.

> **Note**
>
> Si l'en-tête que vous spécifiez n'est pas présent dans la demande, la règle AWS WAF n'est pas du tout appliquée à la demande Web.

Comportement de repli

Lorsque vous utilisez l'adresse IP transférée, vous indiquez le statut de correspondance AWS WAF à attribuer à la requête Web si celle-ci ne possède pas d'adresse IP valide à la position spécifiée :

- MATCH - Traitez la requête Web comme correspondant à l'instruction de règle. AWS WAF applique l'action de règle à la demande.
- AUCUNE CORRESPONDANCE - Traitez la requête Web comme ne correspondant pas à l'instruction de règle.

Adresses IP utilisées dans AWS WAF Bot Control

Le groupe de règles géré par Bot Control vérifie les robots à l'aide des adresses IP provenant de AWS WAF. Si vous utilisez Bot Control et que vous avez vérifié les bots qui acheminent via un proxy ou un équilibreur de charge, vous devez les autoriser explicitement à l'aide d'une règle personnalisée. Par exemple, vous pouvez configurer une règle personnalisée de correspondance des ensembles d'adresses IP qui utilise les adresses IP transférées pour détecter et autoriser vos robots vérifiés. Vous pouvez utiliser cette règle pour personnaliser la gestion de votre bot de différentes manières. Pour plus d'informations et d'exemples, consultez AWS WAF Contrôle des robots.

Considérations générales relatives à l'utilisation des adresses IP transférées

Avant d'utiliser une adresse IP transférée, prenez note des mises en garde générales suivantes :

- Un en-tête peut être modifié par des proxys en cours de route, et les proxys peuvent gérer l'en-tête de différentes manières.
- Les attaquants peuvent modifier le contenu de l'en-tête pour tenter de contourner AWS WAF les inspections.
- L'adresse IP contenue dans l'en-tête peut être mal formée ou non valide.
- L'en-tête que vous spécifiez peut ne pas être présent du tout dans une demande.

Considérations relatives à l'utilisation d'adresses IP transférées avec AWS WAF

La liste suivante décrit les exigences et les mises en garde relatives à l'utilisation d'adresses IP transférées dans : AWS WAF

- Pour chaque règle, vous pouvez spécifier un en-tête pour l'adresse IP transférée. La spécification de l'en-tête ne distingue pas les majuscules et minuscules.

- Pour les instructions de règle basées sur le taux, les instructions de portée imbriquées n'héritent pas de la configuration IP transférée. Spécifiez la configuration de chaque instruction qui utilise une adresse IP transférée.
- Pour les règles de correspondance géographique et basées sur le taux, AWS WAF utilise la première adresse de l'en-tête. Par exemple, si un en-tête contient `10.1.1.1, 127.0.0.0, 10.10.10.10` AWS WAF des `10.1.1.1`
- Pour la correspondance des ensembles d'adresses IP, vous indiquez s'il convient de faire correspondre la première, la dernière ou une adresse quelconque de l'en-tête. Si vous en spécifiez une, AWS WAF inspecte toutes les adresses de l'en-tête pour détecter une correspondance, jusqu'à 10 adresses. Si l'en-tête contient plus de 10 adresses, AWS WAF inspecte les 10 dernières.
- Les en-têtes contenant plusieurs adresses doivent être séparées par des virgules. Si une demande utilise un séparateur autre qu'une virgule, AWS WAF considère que les adresses IP de l'en-tête sont mal formées.
- Si les adresses IP contenues dans l'en-tête sont mal formées ou non valides, AWS WAF indique que la requête Web correspond à la règle ou ne correspond pas, selon le comportement de secours que vous spécifiez dans la configuration IP transférée.
- Si l'en-tête que vous spécifiez n'est pas présent dans une demande, la règle AWS WAF n'y est pas du tout appliquée. Cela signifie que AWS WAF cela n'applique pas l'action de la règle et n'applique pas le comportement de repli.
- Une instruction de règle qui utilise un en-tête IP transféré pour l'adresse IP n'utilisera pas l'adresse IP indiquée par l'origine de la requête Web.

Bonnes pratiques d'utilisation des adresses IP transférées avec AWS WAF

Lorsque vous utilisez des adresses IP transférées, suivez les bonnes pratiques suivantes :

- Examinez attentivement tous les états possibles de vos en-têtes de demande avant d'activer la configuration IP transférée. Il se peut que vous deviez utiliser plusieurs règles pour obtenir le comportement souhaité.
- Pour inspecter plusieurs en-têtes IP transférés ou pour inspecter l'origine de la requête Web et un en-tête IP transféré, utilisez une règle pour chaque source d'adresse IP.
- Pour bloquer les requêtes Web dont l'en-tête n'est pas valide, définissez l'action de règle à bloquer et définissez le comportement de secours correspondant à la configuration IP transférée.

Exemple de code JSON pour les adresses IP transférées

L'instruction de correspondance géographique suivante ne correspond que si l'`X-Forwarded-For`en-tête contient une adresse IP dont le pays d'origine est `US` :

```
{
  "Name": "XFFTestGeo",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "XFFTestGeo"
  },
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ],
      "ForwardedIPConfig": {
        "HeaderName": "x-forwarded-for",
        "FallbackBehavior": "MATCH"
      }
    }
  }
}
```

La règle basée sur le débit suivante agrège les demandes en fonction de la première adresse IP de l'`X-Forwarded-For`en-tête. La règle ne compte que les demandes correspondant à l'instruction de correspondance géographique imbriquée et bloque uniquement les demandes correspondant à l'instruction de correspondance géographique. L'instruction de correspondance géographique imbriquée utilise également l'`X-Forwarded-For`en-tête pour déterminer si l'adresse IP indique le pays d'origine de. `US` Si c'est le cas, ou si l'en-tête est présent mais mal formé, l'instruction geo match renvoie une correspondance.

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

Options pour inspecter les pseudo-en-têtes HTTP/2

Les AWS ressources protégées qui prennent en charge le trafic HTTP/2 ne transmettent pas les pseudo-en-têtes HTTP/2 à des AWS WAF fins d'inspection, mais elles fournissent le contenu des pseudo-en-têtes dans les composants de requête Web qui inspectent. AWS WAF

Vous pouvez l'utiliser AWS WAF pour inspecter uniquement les pseudo-en-têtes répertoriés dans le tableau suivant.

Le contenu du pseudo en-tête HTTP/2 est mappé aux composants de la requête Web

Pseudo-en-tête HTTP/2	Composant de requête Web à inspecter	Documentation

Pseudo-en-tête HTTP/2	Composant de requête Web à inspecter	Documentation
`:method`	Méthode HTTP	Méthode HTTP
`:authority`	En-tête `Host`	En-tête seul Tous les en-têtes
`:path`chemin de l'URI	chemin de l'URI	chemin de l'URI
`:path` query	Chaîne de requête	Chaîne de requête Paramètre de requête unique Tous les paramètres de requête

Options de transformation du texte

Dans les instructions qui recherchent des modèles ou définissent des contraintes, vous pouvez fournir des transformations AWS WAF à appliquer avant d'inspecter la demande. Les transformations de texte éliminent certaines mises en forme inhabituelles que les pirates informatiques utilisent afin de contourner AWS WAF.

Lorsque vous l'utilisez avec la sélection du composant de requête du corps de la requête JSON, AWS WAF applique vos transformations après avoir analysé et extrait les éléments à inspecter à partir du JSON. Pour plus d'informations, consultez corps JSON.

Si vous fournissez plusieurs transformations, vous définissez également l'ordre que AWS WAF doit leur appliquer.

WCU — Chaque transformation de texte correspond à 10 WCU.

La documentation de la AWS WAF console et de l'API fournit également des instructions concernant ces paramètres aux emplacements suivants :

- Générateur de règles sur la console — Transformation de texte. Cette option est disponible lorsque vous utilisez les composants de demande.

- Contenu de la déclaration d'API — `TextTransformations`

Options pour les transformations de texte

Chaque liste de transformation indique les spécifications de la console et de l'API, suivies d'une description.

Base64 decode – `BASE64_DECODE`

AWS WAF décode une chaîne codée en Base64.

Base64 decode extension – `BASE64_DECODE_EXT`

AWS WAF décode une chaîne codée en Base64, mais utilise une implémentation indulgente qui ignore les caractères non valides.

Command line – `CMD_LINE`

Cette option limite les situations dans lesquelles des attaquants pourraient injecter une commande de ligne de commande du système d'exploitation et utiliser un formatage inhabituel pour masquer une partie ou la totalité de la commande.

Utilisez cette option pour exécuter les transformations suivantes :

- Supprimer les caractères suivants : `\ " ' ^`
- Supprimer les espaces avant les caractères suivants : `/ (`
- Remplacer les caractères suivants par un espace : `, ;`
- Remplacer plusieurs espaces par un espace
- Convertir les lettres majuscules `A-Z`, en minuscules, `a-z`

Compress whitespace – `COMPRESS_WHITE_SPACE`

AWS WAF compresse les espaces blancs en remplaçant plusieurs espaces par un espace et en remplaçant les caractères suivants par un espace (ASCII 32) :

- Formfeed (ASCII 12)
- Onglet (ASCII 9)
- Nouvelle ligne (ASCII 10)
- Retour en calèche (ASCII 13)
- Onglet vertical (ASCII 11)
- Espace ininterrompu (ASCII 160)

CSS decode – `CSS_DECODE`

AWS WAF décode les caractères codés à l'aide des règles d'échappement CSS 2.x. `syndata.html#characters` Cette fonction utilise jusqu'à deux octets dans le processus de décodage. Elle peut donc contribuer à découvrir les caractères ASCII qui ont été codés à l'aide d'un codage CSS et qui ne serait généralement pas codés. Elle est également utile pour contrer l'évasion, qui est une combinaison d'une barre oblique inversée et de caractères non hexadécimaux. Par exemple, `ja\vascript` ou `javascript`.

Escape sequences decode – `ESCAPE_SEQ_DECODE`

AWS WAF décode les séquences d'échappement ANSI C suivantes :`\a`,,`\b`,`\f`,`\n`,`\r`,`\t`,`\v`, `\\` `\?\'`, `\xHH` (hexadécimal)`\"`, `\0000` (octal). Les encodages qui ne sont pas valides restent dans la sortie.

Hex decode – `HEX_DECODE`

AWS WAF décode une chaîne de caractères hexadécimaux en binaire.

HTML entity decode – `HTML_ENTITY_DECODE`

AWS WAF remplace les caractères représentés au format hexadécimal `&#xhhhh;` ou au format décimal `&#nnnn;` par les caractères correspondants.

AWS WAF remplace les caractères codés HTML suivants par des caractères non codés. Cette liste utilise un codage HTML en minuscules, mais le traitement ne fait pas la distinction majuscules/minuscules, par exemple, `&QuOt;` et est traitée de la `"` même manière.

Caractère codé en HTML	remplacé par...
`"`	`"`
`&`	`&`
`<`	`<`
`>`	`>`
` ` ou ` `	Espace insécable, décimale 160
`
`	`\n`, décimal 10
` `	`\t`, décimal 9

Caractère codé en HTML	remplacé par...
{ ou {	{
|,	ou		|
} ou }	}
!	!
#	#
$	$
&percent; ou %	%
'	\
(	(
)	)
* ou *	*
+	+
,	,
.	.
/	/
:	:
;	;
=	=
?	?
˜ ou ˜	~

Caractère codé en HTML	remplacé par...
`−`	`-`
`[` ou `[`	`[`
`\`	`\\`
`]` ou `]`	`]`
`&hat;`	`^`
`_` ou `&underbar;`	`_`
`` ou ```	`` ` ``

JS decode – `JS_DECODE`

AWS WAF décode les séquences JavaScript d'échappement. Si un `\uHHHH` code se situe dans la plage de code ASCII pleine largeur de`FF01-FF5E`, l'octet le plus élevé est utilisé pour détecter et ajuster l'octet inférieur. Dans le cas contraire, seul l'octet inférieur est utilisé et l'octet supérieur est mis à zéro, ce qui peut entraîner une perte d'informations.

Lowercase – `LOWERCASE`

AWS WAF convertit les lettres majuscules (A-Z) en minuscules (a-z).

MD5 – `MD5`

AWS WAF calcule un hachage MD5 à partir des données en entrée. Le hachage calculé est au format binaire brut.

None – `NONE`

AWS WAF inspecte la demande Web telle qu'elle a été reçue, sans aucune transformation de texte.

Normalize path – `NORMALIZE_PATH`

AWS WAF normalise la chaîne d'entrée en supprimant les barres obliques multiples, les références automatiques de répertoire et les références arrières de répertoire qui ne se trouvent pas au début de l'entrée.

Normalize path Windows – `NORMALIZE_PATH_WIN`

AWS WAF convertit les barres obliques inverses en barres obliques directes, puis traite la chaîne résultante à l'aide de la transformation. `NORMALIZE_PATH`

Remove nulls – `REMOVE_NULLS`

AWS WAF supprime tous les `NULL` octets de l'entrée.

Replace comments – `REPLACE_COMMENTS`

AWS WAF remplace chaque occurrence d'un commentaire de style C (/*... */) par un seul espace. Il ne compresse pas plusieurs occurrences consécutives. Il remplace les commentaires non terminés par un espace (ASCII 0x20). Cela ne change rien à la fin autonome d'un commentaire (*/).

Replace nulls – `REPLACE_NULLS`

AWS WAF remplace chaque `NULL` octet de l'entrée par le caractère espace (ASCII 0x20).

SQL hex decode – `SQL_HEX_DECODE`

AWS WAF décode les données hexadécimales SQL. Par exemple, AWS WAF décode (`0x414243`) vers (`ABC`).

URL decode – `URL_DECODE`

AWS WAF décode une valeur codée en URL.

URL decode Unicode – `URL_DECODE_UNI`

Comme`URL_DECODE`, mais avec le support du codage spécifique à Microsoft. `%u` Si le code se trouve dans la plage de codes ASCII dans toute sa largeur de `FF01-FF5E`, l'octet supérieur est utilisé pour détecter et ajuster l'octet inférieur. Sinon, seul l'octet inférieur est utilisé et l'octet supérieur est mis à zéro.

UTF8 to Unicode – `UTF8_TO_UNICODE`

AWS WAF convertit toutes les séquences de caractères UTF-8 en Unicode. Cela permet de normaliser la saisie et de minimiser les faux positifs et les faux négatifs pour les langues autres que l'anglais.

Déclarations de portée réduite

Une instruction scope-down est une déclaration de règle imbriquable que vous ajoutez dans une déclaration de groupe de règles géré ou une instruction basée sur le taux afin de limiter l'ensemble

de demandes évaluées par la règle correspondante. La règle contenante évalue uniquement les demandes qui correspondent en premier lieu à l'instruction scope-down.

- Déclaration de groupe de règles géré : si vous ajoutez une instruction de portée réduite à une déclaration de groupe de règles géré, toute demande ne AWS WAF correspondant pas à l'instruction de portée réduite est considérée comme ne correspondant pas au groupe de règles. Seules les demandes correspondant à l'instruction scope-down sont évaluées par rapport au groupe de règles. Pour les groupes de règles gérés dont la tarification est basée sur le nombre de demandes évaluées, les instructions de délimitation peuvent aider à contenir les coûts.

  Pour plus d'informations sur les instructions de groupes de règles gérés, consultezInstruction de groupe de règles géré.
- Déclaration de règle basée sur le taux — Une déclaration de règle basée sur le taux sans indication de portée vers le bas limite toutes les demandes évaluées par la règle. Si vous souhaitez uniquement contrôler le taux pour une catégorie spécifique de demandes, ajoutez une instruction de portée réduite à la règle basée sur le taux. Par exemple, pour suivre et contrôler uniquement le taux de demandes provenant d'une zone géographique spécifique, vous pouvez spécifier cette zone géographique dans une déclaration de correspondance géographique et l'ajouter à votre règle basée sur les taux en tant que déclaration de délimitation.

  Pour plus d'informations sur les instructions de règles basées sur les taux, consultezInstruction de règle basée sur un taux.

Vous pouvez utiliser n'importe quelle règle imbriquable dans une instruction scope-down. Pour les relevés disponibles, voir Faire correspondre les déclarations des règles etDéclarations de règles logiques. Les WCU pour une instruction scope-down sont les WCU requis pour l'instruction de règle que vous y définissez. Il n'y a aucun coût supplémentaire pour l'utilisation d'une déclaration de portée réduite.

Vous pouvez configurer une instruction scope-down de la même manière que lorsque vous utilisez l'instruction dans une règle normale. Par exemple, vous pouvez appliquer des transformations de texte à un composant de requête Web que vous inspectez et vous pouvez spécifier une adresse IP transférée à utiliser comme adresse IP. Ces configurations s'appliquent uniquement à l'instruction scope-down et ne sont pas héritées par le groupe de règles géré ou l'instruction de règle basée sur le taux qui les contient.

Par exemple, si vous appliquez des transformations de texte à une chaîne de requête dans votre instruction scope-down, l'instruction scope-down inspecte la chaîne de requête après avoir appliqué

les transformations. Si la demande répond aux critères de l'instruction scope-down, AWS WAF elle transmet la demande Web à la règle conteneur dans son état d'origine, sans les transformations de l'instruction scope-down. La règle qui contient l'instruction scope-down peut appliquer ses propres transformations de texte, mais elle n'hérite aucune de l'instruction scope-down.

Vous ne pouvez pas utiliser une instruction scope-down pour spécifier une configuration d'inspection des demandes pour l'instruction de règle qui la contient. Vous ne pouvez pas utiliser une instruction scope-down comme préprocesseur de requête Web pour l'instruction de règle qui la contient. Le seul rôle d'une instruction scope-down est de déterminer quelles demandes sont transmises à l'instruction de règle la contenant pour inspection.

Instructions faisant référence à un ensemble ou à un groupe de règles

Certaines règles utilisent des entités réutilisables et gérées en dehors de vos ACL Web, soit par vous AWS, soit par un AWS Marketplace vendeur. Lorsque l'entité réutilisable est mise à jour, AWS WAF propage la mise à jour à votre règle. Par exemple, si vous utilisez un groupe de règles AWS gérées dans une ACL Web, lors de la AWS mise à jour du groupe de règles, la modification est AWS propagée à votre ACL Web afin de mettre à jour son comportement. Si vous utilisez une instruction IP set dans une règle, lorsque vous mettez à jour l'ensemble, la modification est AWS WAF répercutée sur toutes les règles qui y font référence, de sorte que toutes les ACL Web qui utilisent ces règles sont conservées up-to-date avec vos modifications.

Voici les entités réutilisables que vous pouvez utiliser dans une instruction de règle.

- Ensembles d'adresses IP — Vous créez et gérez vos propres ensembles d'adresses IP. Sur la console, vous pouvez y accéder à partir du volet de navigation. Pour de plus amples informations sur la gestion des jeux d'adresses IP, reportez-vous à la section Ensembles d'adresses IP et ensembles de modèles regex dans AWS WAF.
- Sets de matchs regex — Vous créez et gérez vos propres sets de matchs regex. Sur la console, vous pouvez y accéder à partir du volet de navigation. Pour de plus amples informations sur la gestion des ensembles de modèles regex, reportez-vous à la section Ensembles d'adresses IP et ensembles de modèles regex dans AWS WAF.
- AWS Groupes de règles gérées : AWS gère ces groupes de règles. Sur la console, ceux-ci sont disponibles pour votre utilisation lorsque vous ajoutez un groupe de règles gérées à votre liste ACL web. Pour de plus amples informations, veuillez consulter AWS Liste des groupes de règles gérées.
- AWS Marketplace groupes de règles gérés : AWS Marketplace les vendeurs gèrent ces groupes de règles et vous pouvez vous y abonner pour les utiliser. Pour gérer vos abonnements, dans

le volet de navigation de la console, sélectionnez AWS Marketplace. Les groupes de règles AWS Marketplace gérés sont répertoriés lorsque vous ajoutez un groupe de règles géré à votre ACL Web. Pour les groupes de règles auxquels vous n'êtes pas encore abonné, vous trouverez également un lien vers AWS Marketplace ces groupes sur cette page. Pour plus d'informations sur les groupes de règles gérés par le AWS Marketplace vendeur, consultezAWS Marketplace groupes de règles gérés.

- Vos propres groupes de règles : vous gérez vos propres groupes de règles, généralement lorsque vous avez besoin d'un comportement qui n'est pas disponible dans les groupes de règles gérés. Sur la console, vous pouvez y accéder à partir du volet de navigation. Pour plus d'informations, consultez Gestion de vos propres groupes de règles.

Suppression d'un jeu ou d'un groupe de règles référencé

Lorsque vous supprimez une entité référencée AWS WAF , vérifiez si elle est actuellement utilisée dans une ACL Web. S'il AWS WAF découvre qu'il est en cours d'utilisation, il vous avertit. AWS WAF est presque toujours capable de déterminer si une entité est référencée par une ACL Web. Cependant, dans de rares cas, il pourrait ne pas être en mesure de le faire. Si vous devez vous assurer que l'entité que vous souhaitez supprimer n'est pas en cours d'utilisation, vérifiez qu'elle est dans vos listes ACL web avant de la supprimer.

Faire correspondre les déclarations des règles

Les instructions Match comparent la demande Web ou son origine aux critères que vous fournissez. Pour de nombreuses instructions de ce type, AWS WAF compare un composant spécifique de la demande de contenu correspondant.

Les relevés de match sont imbriquables. Vous pouvez imbriquer n'importe laquelle de ces instructions dans des instructions de règles logiques et vous pouvez les utiliser dans des instructions de portée réduite. Pour plus d'informations sur les instructions de règles logiques, consultezDéclarations de règles logiques. Pour plus d'informations sur les instructions de portée réduite, voir. Déclarations de portée réduite

Ce tableau décrit les instructions de correspondance régulières que vous pouvez ajouter à une règle et fournit des directives pour calculer l'utilisation des unités de capacité ACL (WCU) Web pour chacune d'entre elles. Pour de plus amples informations sur les WCU, veuillez consulter AWS WAF unités de capacité ACL Web (WCU).

Déclaration de correspondance	Description	WCU
Correspondance géographique	Inspecte le pays d'origine de la demande et applique des étiquettes pour le pays et la région d'origine.	1
Correspondance d'ensemble d'adresses IP	Inspecte la demande par rapport à un ensemble d'adresses IP et de plages d'adresses.	1 dans la plupart des cas. Si vous configurez l'instruction pour utiliser un en-tête avec des adresses IP transférées et que vous spécifiez une position dans l'en-tête deAny, augmentez le nombre de WCU de 4.
Déclaration relative à la règle de correspondance des étiquettes	Inspecte la demande pour les étiquettes qui ont été ajoutées par d'autres règles dans la même ACL Web.	1
Déclaration de règle de correspondance Regex	Compare un modèle de regex avec un composant de requête spécifié.	3, comme coût de base. Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.
Ensemble de modèles Regex		25 par jeu de modèles, comme coût de base.

Déclaration de correspondance	Description	WCU
	Compare les modèles regex à un composant de requête spécifié.	Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.
Contrainte de taille	Vérifie les contraintes de taille par rapport à un composant de demande spécifié.	1, comme coût de base. Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.
Attaque SQLi	Inspecte la présence de code SQL malveillant dans un composant de requête spécifié.	20, comme coût de base. Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.

Déclaration de correspondance	Description	WCU
Correspondance de chaîne	Compare une chaîne à un composant de demande spécifié.	Le coût de base dépend du type de correspondance de chaîne et se situe entre 1 et 10. Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.
Attaque par scripts XSS	Inspecte les attaques de script intersite dans un composant de demande spécifié.	40, comme coût de base. Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.

Instruction de correspondance géographique de règle

Utilisez des déclarations géographiques ou de correspondance géographique pour gérer les demandes Web en fonction du pays et de la région d'origine. Une déclaration de correspondance géographique ajoute aux requêtes Web des étiquettes indiquant le pays d'origine et la région d'origine. Il ajoute ces étiquettes, que les critères de l'énoncé correspondent ou non à la demande.

Une instruction de correspondance géographique effectue également une correspondance avec le pays d'origine de la demande.

Comment utiliser la déclaration Geo Match

Vous pouvez utiliser l'instruction Geo Match pour faire correspondre un pays ou une région, comme suit :

- Pays — Vous pouvez utiliser une règle de correspondance géographique à elle seule pour gérer les demandes uniquement en fonction de leur pays d'origine. L'énoncé de règle correspond aux codes de pays. Vous pouvez également suivre une règle de correspondance géographique avec une règle de correspondance d'étiquette qui correspond à l'étiquette du pays d'origine.
- Région : utilisez une règle de correspondance géographique suivie d'une règle de correspondance d'étiquettes pour gérer les demandes en fonction de leur région d'origine. Vous ne pouvez pas utiliser une règle de correspondance géographique uniquement pour établir une correspondance avec des codes de région.

Pour plus d'informations sur l'utilisation des règles de correspondance des étiquettes, reportez-vous aux Déclaration relative à la règle de correspondance des étiquettes sections etAWS WAF étiquettes sur les requêtes Web.

Comment fonctionne la déclaration Geo Match

Avec l'instruction geo match, AWS WAF gère chaque requête Web comme suit :

1. Détermine les codes de pays et de région de la demande : AWS WAF détermine le pays et la région d'une demande en fonction de son adresse IP. Par défaut, AWS WAF utilise l'adresse IP d'origine de la requête Web. Vous pouvez demander d' AWS WAF utiliser une adresse IP provenant d'un autre en-tête de demande`X-Forwarded-For`, par exemple en activant la configuration IP transférée dans les paramètres de l'instruction de règle.

   AWS WAF détermine l'emplacement des demandes à l'aide des bases de MaxMind données GeoIP. MaxMind fait état d'une très grande précision de ses données au niveau des pays, bien que la précision varie en fonction de facteurs tels que le pays et le type de propriété intellectuelle. Pour plus d'informations MaxMind, consultez la section Géolocalisation MaxMind IP. Si vous pensez que l'une des données GeoIP est incorrecte, vous pouvez envoyer une demande de correction à Maxmind à l'adresse MaxMind Correct GeoIP2 Data.

AWS WAF utilise les codes de pays et de région alpha-2 de la norme 3166 de l'Organisation internationale de normalisation (ISO). Vous pouvez trouver les codes aux endroits suivants :

- Sur le site Web de l'ISO, vous pouvez rechercher les codes de pays sur la plateforme de navigation en ligne ISO (OBP).
- Sur Wikipédia, les codes de pays sont répertoriés selon la norme ISO 3166-2.

  Les codes régionaux d'un pays sont répertoriés dans l'URL`https://en.wikipedia.org/wiki/ISO_3166-2:`*`<ISO country code>`*. Par exemple, les régions des États-Unis sont conformes à la norme ISO 3166-2:US et celles de l'Ukraine à la norme ISO 3166-2:UA.

2. Détermine le libellé du pays et le libellé de la région à ajouter à la demande : les étiquettes indiquent si l'instruction Geo Match utilise l'adresse IP d'origine ou une configuration IP transférée.

   - IP d'origine

     L'étiquette du pays est`awswaf:clientip:geo:country:`*`<ISO country code>`*. Exemple pour les États-Unis :`awswaf:clientip:geo:country:US`.

     L'étiquette de la région est`awswaf:clientip:geo:region:`*`<ISO country code>`*`-`*`<ISO region code>`*. Exemple pour l'Oregon aux États-Unis :`awswaf:clientip:geo:region:US-OR`.

   - IP transférée

     L'étiquette du pays est`awswaf:forwardedip:geo:country:`*`<ISO country code>`*. Exemple pour les États-Unis :`awswaf:forwardedip:geo:country:US`.

     L'étiquette de la région est`awswaf:forwardedip:geo:region:`*`<ISO country code>`*`-`*`<ISO region code>`*. Exemple pour l'Oregon aux États-Unis :`awswaf:forwardedip:geo:region:US-OR`.

   Si le code de pays ou de région n'est pas disponible pour l'adresse IP spécifiée dans une demande, AWS WAF `XX` utilisez-le dans les libellés, à la place de la valeur. Par exemple, l'étiquette suivante est pour une adresse IP client dont le code de pays n'est pas disponible : `awswaf:clientip:geo:country:XX` et l'étiquette suivante est pour une adresse IP transférée dont le pays est les États-Unis, mais dont le code de région n'est pas disponible :`awswaf:forwardedip:geo:region:US-XX`.

3. Évalue le code de pays de la demande par rapport aux critères de la règle

L'instruction Geo Match ajoute des libellés de pays et de régions à toutes les demandes qu'elle inspecte, qu'elle trouve ou non une correspondance.

> **Note**
>
> AWS WAF ajoute des libellés à la fin de l'évaluation des requêtes Web d'une règle. Pour cette raison, toute étiquette que vous utilisez par rapport aux libellés d'une instruction de correspondance géographique doit être définie dans une règle distincte de celle qui contient l'instruction de correspondance géographique.

Si vous souhaitez inspecter uniquement les valeurs des régions, vous pouvez écrire une règle de correspondance géographique avec une Count action et une seule correspondance de code de pays, suivie d'une règle de correspondance d'étiquettes pour les étiquettes de région. Vous devez fournir un code de pays pour que la règle de correspondance géographique puisse être évaluée, même pour cette approche. Vous pouvez réduire les statistiques de journalisation et de comptage en spécifiant un pays qui est très peu susceptible d'être une source de trafic vers votre site.

CloudFront les distributions et la CloudFront fonction de restriction géographique

Pour les CloudFront distributions, si vous utilisez la fonctionnalité CloudFront de restriction géographique, sachez que cette fonctionnalité ne transmet pas les demandes bloquées à AWS WAF. Il transmet les demandes autorisées à AWS WAF. Si vous souhaitez bloquer les demandes en fonction de la géographie et d'autres critères que vous pouvez spécifier AWS WAF, utilisez l'instruction AWS WAF de correspondance géographique et n'utilisez pas la fonctionnalité CloudFront de restriction géographique.

Caractéristiques de Geo Match Statement

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCU — 1 WCU.

Paramètres — Cette instruction utilise les paramètres suivants :

- Codes de pays : ensemble de codes de pays à comparer pour une correspondance géographique. Il doit s'agir de codes de pays à deux caractères issus des codes ISO de pays alpha-2 de la norme internationale ISO 3166, par exemple. `["US","CN"]`
- (Facultatif) Configuration IP transférée — Par défaut, AWS WAF utilise l'adresse IP dans l'origine de la requête Web pour déterminer le pays d'origine. Vous pouvez également configurer la règle

pour utiliser une adresse IP transférée dans un en-tête HTTP à la `X-Forwarded-For` place. AWS WAF utilise la première adresse IP de l'en-tête. Avec cette configuration, vous spécifiez également un comportement de secours à appliquer à une requête Web dont l'en-tête contient une adresse IP mal formée. Le comportement de remplacement définit le résultat correspondant à la demande, qu'il corresponde ou non. Pour plus d'informations, consultez Adresse IP transférée.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour l'option Demande, choisissez Provient d'un pays de.
- API — GeoMatchStatement

Exemples

Vous pouvez utiliser le relevé de correspondance géographique pour gérer les demandes provenant de pays ou de régions spécifiques. Par exemple, si vous souhaitez bloquer les demandes provenant de certains pays, tout en autorisant les demandes provenant d'un ensemble spécifique d'adresses IP dans ces pays, vous pouvez créer une règle avec l'action définie sur Block et les instructions imbriquées suivantes, affichées en pseudocode :

- AND déclaration
  - Instruction de correspondance géographique répertoriant les pays que vous souhaitez bloquer
  - NOT déclaration
    - Instruction de jeu d'adresses IP qui spécifie les adresses IP via lesquelles vous souhaitez autoriser

Ou, si vous souhaitez bloquer certaines régions dans certains pays, tout en autorisant les demandes provenant d'autres régions de ces pays, vous pouvez d'abord définir une règle de correspondance géographique avec l'action définie sur. Count Définissez ensuite une règle de correspondance d'étiquettes qui correspond aux étiquettes de correspondance géographique ajoutées et gère les demandes selon vos besoins.

Le pseudo-code suivant décrit un exemple de cette approche :

1. Déclaration de correspondance géographique répertoriant les pays dont les régions que vous souhaitez bloquer, mais dont l'action est définie sur Compter. Cela étiquette chaque demande Web quel que soit le statut de correspondance, et vous donne également des mesures de comptage pour les pays qui vous intéressent.

2. ANDdéclaration avec action de blocage
   - Déclaration de correspondance des libellés qui spécifie les libellés des pays que vous souhaitez bloquer
   - NOT déclaration
     - Déclaration de correspondance des étiquettes qui spécifie les libellés des régions des pays que vous souhaitez autoriser à passer

La liste JSON suivante montre une implémentation des deux règles décrites dans le pseudocode précédent. Ces règles bloquent tout le trafic en provenance des États-Unis, à l'exception du trafic en provenance de l'Oregon et de Washington. La déclaration Geo Match ajoute des étiquettes de pays et de régions à toutes les demandes qu'elle inspecte. La règle de correspondance des libellés s'exécute après la règle de correspondance géographique, de sorte qu'elle peut correspondre aux étiquettes de pays et de régions que la règle de correspondance géographique vient d'ajouter. L'instruction Geo Match utilise une adresse IP transférée, de sorte que la correspondance d'étiquettes spécifie également les étiquettes IP transférées.

```
{
   "Name": "geoMatchForLabels",
   "Priority": 10,
   "Statement": {
     "GeoMatchStatement": {
       "CountryCodes": [
         "US"
       ],
       "ForwardedIPConfig": {
           "HeaderName": "X-Forwarded-For",
           "FallbackBehavior": "MATCH"
       }
     }
   },
   "Action": {
     "Count": {}
   },
   "VisibilityConfig": {
     "SampledRequestsEnabled": true,
     "CloudWatchMetricsEnabled": true,
     "MetricName": "geoMatchForLabels"
   }
},
{
```

```
  "Name": "blockUSButNotOROrWA",
  "Priority": 11,
  "Statement": {
    "AndStatement": {
      "Statements": [
        {
          "LabelMatchStatement": {
            "Scope": "LABEL",
            "Key": "awswaf:forwardedip:geo:country:US"
          }
        },
        {
          "NotStatement": {
            "Statement": {
               "OrStatement": {
                 "Statements": [
                   {
                      "LabelMatchStatement": {
                        "Scope": "LABEL",
                        "Key": "awswaf:forwardedip:geo:region:US-OR"
                      }
                   },
                   {
                      "LabelMatchStatement": {
                        "Scope": "LABEL",
                        "Key": "awswaf:forwardedip:geo:region:US-WA"
                      }
                   }
                 ]
               }
            }
          }
        }
      ]
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "blockUSButNotOROrWA"
  }
```

```
}
```

Autre exemple, vous pouvez associer la géolocalisation à des règles basées sur les taux afin de hiérarchiser les ressources destinées aux utilisateurs d'un pays ou d'une région en particulier. Vous créez un relevé tarifaire différent pour chaque relevé de correspondance géographique ou de correspondance d'étiquette que vous utilisez pour différencier vos utilisateurs. Définissez une limite de débit supérieure pour les utilisateurs du pays ou de la région de votre choix et définissez une limite de débit inférieure pour les autres utilisateurs.

La liste JSON suivante montre une règle de correspondance géographique suivie de règles basées sur le taux qui limitent le débit du trafic en provenance des États-Unis. Les règles permettent au trafic en provenance de l'Oregon d'entrer à un rythme plus élevé que le trafic en provenance de n'importe quel autre endroit du pays.

```
{
  "Name": "geoMatchForLabels",
  "Priority": 190,
  "Statement": {
    "GeoMatchStatement": {
      "CountryCodes": [
        "US"
      ]
    }
  },
  "Action": {
    "Count": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "geoMatchForLabels"
  }
},
{
  "Name": "rateLimitOregon",
  "Priority": 195,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 3000,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "LabelMatchStatement": {
```

```
          "Scope": "LABEL",
          "Key": "awswaf:clientip:geo:region:US-OR"
        }
      }
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitOregon"
  }
},
{
  "Name": "rateLimitUSNotOR",
  "Priority": 200,
  "Statement": {
    "RateBasedStatement": {
      "Limit": 100,
      "AggregateKeyType": "IP",
      "ScopeDownStatement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:clientip:geo:country:US"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:clientip:geo:region:US-OR"
                  }
                }
              }
            }
          ]
        }
      }
```

```
    }
  },
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "rateLimitUSNotOR"
  }
}
```

Instruction de correspondance d'ensemble d'adresses IP de règle

L'instruction IP set match inspecte l'adresse IP d'une requête Web par rapport à un ensemble d'adresses IP et de plages d'adresses. Utilisez cette option pour autoriser ou bloquer les demandes web basées sur les adresses IP d'origine des demandes. Par défaut, AWS WAF utilise l'adresse IP de l'origine de la requête Web, mais vous pouvez configurer la règle pour utiliser un en-tête HTTP à la `X-Forwarded-For` place.

AWS WAF prend en charge toutes les plages d'adresses CIDR IPv4 et IPv6, à l'exception de. `/0` Pour plus d'informations sur la notation CIDR, consultez l'article Classless Inter-Domain Routing sur Wikipédia (en anglais). Un jeu d'adresses IP peut contenir jusqu'à 10 000 adresses IP ou plages d'adresses IP à vérifier.

> **Note**
>
> Chaque règle de correspondance de jeu d'adresses IP fait référence à un jeu d'adresses IP que vous créez et conservez indépendamment de vos règles. Vous pouvez utiliser un seul ensemble d'adresses IP dans plusieurs règles, et lorsque vous mettez à jour l'ensemble référencé, toutes les règles qui y font référence AWS WAF sont automatiquement mises à jour.
>
> Pour plus d'informations sur la création et la gestion d'un ensemble d'adresses IP, consultezCréation et gestion d'un ensemble d'adresses IP.

Lorsque vous ajoutez ou mettez à jour les règles dans votre groupe de règles ou votre liste ACL web, choisissez l'option Jeu d'adresses IP et sélectionnez le nom du jeu d'adresses IP que vous souhaitez utiliser.

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCU — 1 WCU pour la plupart. Si vous configurez l'instruction pour utiliser les adresses IP transférées et que vous spécifiez une position deANY, augmentez l'utilisation de la WCU de 4.

Cette instruction utilise les paramètres suivants :

- Spécification de l'ensemble d'adresses IP — Choisissez l'ensemble d'adresses IP que vous souhaitez utiliser dans la liste ou créez-en un nouveau.
- (Facultatif) Configuration IP transférée : nom d'en-tête IP transféré alternatif à utiliser à la place de l'origine de la demande. Vous spécifiez si la correspondance doit être faite avec la première, la dernière ou avec n'importe quelle adresse de l'en-tête. Vous spécifiez également un comportement de secours à appliquer à une requête Web dont l'adresse IP est mal formée dans l'en-tête spécifié. Le comportement de remplacement définit le résultat correspondant à la demande, qu'il corresponde ou non. Pour plus d'informations, consultez Adresse IP transférée.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour l'option Requête, choisissez Provient d'une adresse IP dans.
- Ajouter mes propres règles et groupes de règles sur la console — Choisissez l'option IP set.
- API — IP SetReferenceStatement

Déclaration relative à la règle de correspondance des étiquettes

L'instruction label match inspecte les étiquettes figurant sur la requête Web par rapport à une spécification de chaîne. Les étiquettes disponibles pour une règle à des fins d'inspection sont celles qui ont déjà été ajoutées à la requête Web par d'autres règles dans le cadre de la même évaluation ACL Web.

Les étiquettes ne sont pas conservées en dehors de l'évaluation de l'ACL Web, mais vous pouvez accéder aux métriques des étiquettes CloudWatch et vous pouvez voir des résumés des informations relatives aux étiquettes pour n'importe quelle ACL Web dans la AWS WAF console. Pour plus d'informations, consultez Métriques et dimensions des étiquettes et Surveillance et réglage. Vous pouvez également voir les étiquettes dans les journaux. Pour plus d'informations, consultez Champs de journal.

> **Note**
>
> Une instruction de correspondance d'étiquettes ne peut voir que les libellés issus de règles précédemment évaluées dans l'ACL Web. Pour plus d'informations sur le AWS WAF mode d'évaluation des règles et des groupes de règles dans une ACL Web, consultezOrdre de traitement des règles et des groupes de règles dans une ACL Web.

Pour plus d'informations sur l'ajout et la mise en correspondance d'étiquettes, consultezAWS WAF étiquettes sur les requêtes Web.

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCU — 1 ECU

Cette instruction utilise les paramètres suivants :

- Champ de correspondance : définissez ce paramètre sur Label pour qu'il corresponde au nom de l'étiquette et, éventuellement, aux espaces de noms et au préfixe précédents. Définissez ce paramètre sur Namespace pour qu'il corresponde à certaines ou à toutes les spécifications de l'espace de noms et, éventuellement, au préfixe précédent.
- Clé — La chaîne à laquelle vous souhaitez faire correspondre. Si vous spécifiez une étendue de correspondance d'espaces de noms, celle-ci ne doit spécifier que les espaces de noms et éventuellement le préfixe, avec deux points à la fin. Si vous spécifiez une étendue de correspondance d'étiquettes, celle-ci doit inclure le nom de l'étiquette et peut éventuellement inclure les espaces de noms et le préfixe précédents.

Pour plus d'informations sur ces paramètres, consultez AWS WAF règles qui correspondent aux libellés et AWS WAF exemples de correspondance d'étiquettes.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour l'option Demande, choisissez Has label.
- API — LabelMatchStatement

Déclaration de règle de correspondance Regex

Une instruction regex match indique de AWS WAF faire correspondre un composant de requête à une seule expression régulière (regex). Une requête Web correspond à l'instruction si le composant de demande correspond à l'expression régulière que vous spécifiez.

Ce type d'instruction constitue une bonne alternative Instruction de correspondance d'ensemble de modèles d'expression régulière de règle aux situations dans lesquelles vous souhaitez combiner vos critères de correspondance en utilisant la logique mathématique. Par exemple, si vous souhaitez qu'un composant de requête corresponde à certains modèles de regex et non à d'autres, vous pouvez combiner les instructions regex match en utilisant le ANDdéclaration de règle et le. NOTdéclaration de règle

AWS WAF prend en charge la syntaxe des modèles utilisée par la bibliothèque PCRE, `libpcre` à quelques exceptions près. La bibliothèque est documentée sur PCRE - Perl Compatible Regular Expressions. Pour plus d'informations sur AWS WAF le support, consultezModèle d'expression régulière correspondant dans AWS WAF.

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCU — 3 WCU, comme coût de base. Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.

Ce type d'instruction fonctionne sur un composant de requête Web et nécessite les paramètres de composant de demande suivants :

- Composant de demande : partie de la requête Web destinée à inspecter, par exemple, une chaîne de requête ou le corps de la requête.

  > **Warning**
  >
  > Si vous inspectez les composants de la requête Body, JSON body, Headers ou Cookies, renseignez-vous sur les limites relatives à Gestion des composants de demande surdimensionnés dans AWS WAF la quantité de contenu AWS WAF pouvant être inspectée.

  Pour plus d'informations sur les composants des requêtes Web, consultezSpécification et gestion des composants de requête Web.

- Transformations de texte facultatives : transformations que vous AWS WAF souhaitez effectuer sur le composant de demande avant de l'inspecter. Par exemple, vous pouvez passer en minuscules ou normaliser les espaces blancs. Si vous spécifiez plusieurs transformations, AWS WAF traitez-les dans l'ordre indiqué. Pour plus d'informations, consultez Options de transformation du texte.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour le type Match, choisissez Correspond à une expression régulière.
- API — RegexMatchStatement

Instruction de correspondance d'ensemble de modèles d'expression régulière de règle

La correspondance de l'ensemble de modèles regex inspecte la partie de la demande web que vous spécifiez et recherche les modèles d'expression régulière que vous avez définis dans un ensemble de modèles regex.

AWS WAF prend en charge la syntaxe des modèles utilisée par la bibliothèque PCRE, `libpcre` à quelques exceptions près. La bibliothèque est documentée sur PCRE - Perl Compatible Regular Expressions. Pour plus d'informations sur AWS WAF le support, consultezModèle d'expression régulière correspondant dans AWS WAF.

> **Note**
>
> Chaque règle de correspondance d'ensemble de modèles regex fait référence à un ensemble de modèlesregex, que vous créez et maintenez indépendamment de vos règles. Vous pouvez utiliser un seul ensemble de modèles regex dans plusieurs règles, et lorsque vous mettez à jour l'ensemble référencé, toutes les règles qui y font référence AWS WAF sont automatiquement mises à jour.
>
> Pour de plus amples informations sur la création et la gestion d'un ensemble de modèles regex, reportez-vous à la section Création et gestion d'un ensemble de modèles d'expression régulière.

Une instruction regex pattern set match indique de AWS WAF rechercher l'un des modèles de l'ensemble dans le composant de requête que vous choisissez. Une demande web correspond à

l'instruction de règle de l'ensemble de modèles si le composant de demande correspond à l'un des modèles de l'ensemble.

Si vous souhaitez combiner vos correspondances de modèles regex en utilisant la logique, par exemple pour les faire correspondre à certaines expressions régulières et non à d'autres, pensez à utiliserDéclaration de règle de correspondance Regex.

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCU — 25 WCU, comme coût de base. Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.

Ce type d'instruction fonctionne sur un composant de requête Web et nécessite les paramètres de composant de demande suivants :

- Composant de demande : partie de la requête Web destinée à inspecter, par exemple, une chaîne de requête ou le corps de la requête.

  > ⚠ Warning
  >
  > Si vous inspectez les composants de la requête Body, JSON body, Headers ou Cookies, renseignez-vous sur les limites relatives à Gestion des composants de demande surdimensionnés dans AWS WAF la quantité de contenu AWS WAF pouvant être inspectée.

  Pour plus d'informations sur les composants des requêtes Web, consultezSpécification et gestion des composants de requête Web.
- Transformations de texte facultatives : transformations que vous AWS WAF souhaitez effectuer sur le composant de demande avant de l'inspecter. Par exemple, vous pouvez passer en minuscules ou normaliser les espaces blancs. Si vous spécifiez plusieurs transformations, AWS WAF traitez-les dans l'ordre indiqué. Pour plus d’informations, consultez Options de transformation du texte.

Cette instruction nécessite les paramètres suivants :

- Spécification du jeu de modèles Regex — Choisissez le jeu de modèles Regex que vous souhaitez utiliser dans la liste ou créez-en un nouveau.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour Type de correspondance, choisissez Condition de correspondance de chaîne > Correspond au modèle du jeu d'expressions régulières.
- API — RegexPatternSetReferenceStatement

Instruction de contrainte de taille de règle

Une instruction de contrainte de taille compare le nombre d'octets d'un composant de requête Web à un nombre que vous fournissez, et le fait correspondre en fonction de vos critères de comparaison. Le critère de comparaison est un opérateur tel que supérieur à (>) ou inférieur à (<). Par exemple, vous pouvez établir une correspondance sur des demandes dont la taille de la chaîne de requête est supérieure à 100 octets.

> **Note**
>
> Cette instruction inspecte uniquement la taille du composant de requête Web. Il n'inspecte pas le contenu du composant.

Si vous inspectez le chemin de l'URI, tout / élément du chemin compte pour un caractère. Par exemple, le chemin `/logo.jpg` de l'URI comporte neuf caractères.

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCU — 1 WCU, comme coût de base. Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.

Ce type d'instruction fonctionne sur un composant de requête Web et nécessite les paramètres de composant de demande suivants :

- Composant de demande : partie de la requête Web destinée à inspecter, par exemple, une chaîne de requête ou le corps de la requête. Pour plus d'informations sur les composants des requêtes Web, consultezSpécification et gestion des composants de requête Web.

  Une instruction de contrainte de taille inspecte uniquement la taille du composant une fois les transformations appliquées. Il n'inspecte pas le contenu du composant.

- Transformations de texte facultatives : transformations que vous AWS WAF souhaitez effectuer sur le composant de demande avant d'inspecter sa taille. Par exemple, vous pouvez compresser des espaces blancs ou décoder des entités HTML. Si vous spécifiez plusieurs transformations, AWS WAF traitez-les dans l'ordre indiqué. Pour plus d'informations, consultez Options de transformation du texte.

En outre, cette instruction nécessite les paramètres suivants :

- Condition de correspondance de taille : indique l'opérateur de comparaison numérique à utiliser pour comparer la taille que vous fournissez avec le composant de demande que vous avez choisi. Choisissez l'opérateur dans la liste.
- Taille : paramètre de taille, en octets, à utiliser dans la comparaison.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour Type de correspondance, sous Condition de correspondance de taille, choisissez la condition que vous souhaitez utiliser.
- API — SizeConstraintStatement

Instruction d'attaque par injection SQL de règle

Une instruction de règle d'injection SQL permet de détecter la présence de code SQL malveillant. Les attaquants insèrent du code SQL malveillant dans les requêtes Web afin de modifier votre base de données ou d'en extraire des données.

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCU — Le coût de base dépend du niveau de sensibilité défini pour l'énoncé de règle : Low coûte 20 et High coûte 30.

Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.

Ce type d'instruction fonctionne sur un composant de requête Web et nécessite les paramètres de composant de demande suivants :

- Composant de demande : partie de la requête Web destinée à inspecter, par exemple, une chaîne de requête ou le corps de la requête.

  > **Warning**
  >
  > Si vous inspectez les composants de la requête Body, JSON body, Headers ou Cookies, renseignez-vous sur les limites relatives à Gestion des composants de demande surdimensionnés dans AWS WAF la quantité de contenu AWS WAF pouvant être inspectée.

  Pour plus d'informations sur les composants des requêtes Web, consultezSpécification et gestion des composants de requête Web.

- Transformations de texte facultatives : transformations que vous AWS WAF souhaitez effectuer sur le composant de demande avant de l'inspecter. Par exemple, vous pouvez passer en minuscules ou normaliser les espaces blancs. Si vous spécifiez plusieurs transformations, AWS WAF traitez-les dans l'ordre indiqué. Pour plus d’informations, consultez Options de transformation du texte.

En outre, cette instruction nécessite le réglage suivant :

- Niveau de sensibilité : ce paramètre ajuste la sensibilité des critères de correspondance par injection SQL. Les options sont LOW et HIGH. Le paramètre par défaut est LOW.

  Le HIGH paramètre détecte un plus grand nombre d'attaques par injection SQL et est le paramètre recommandé. En raison de la sensibilité accrue, ce paramètre génère davantage de faux positifs, en particulier si vos requêtes Web contiennent généralement des chaînes inhabituelles. Au cours du test et du réglage de votre ACL Web, vous devrez peut-être redoubler d'efforts pour atténuer les faux positifs. Pour plus d’informations, consultez Tester et ajuster vos AWS WAF protections.

  La valeur la plus faible permet une détection des injections SQL moins rigoureuse, ce qui réduit également le nombre de faux positifs. LOWpeut être un meilleur choix pour les ressources dotées d'autres protections contre les attaques par injection de code SQL ou présentant une faible tolérance aux faux positifs.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour Type de match, choisissez Attack match condition > Contient des attaques par injection SQL.
- API — SqliMatchStatement

Instruction de correspondance de chaîne de règle

Une instruction de correspondance de chaîne indique la chaîne que vous AWS WAF souhaitez rechercher dans une demande, son emplacement dans la demande et le mode de recherche. Par exemple, vous pouvez rechercher une chaîne spécifique au début de n'importe quelle chaîne de requête de la demande ou comme correspondance exacte pour l'en-tête `User-agent` de la demande. Généralement, la chaîne est composée de caractères ASCII affichables, mais vous pouvez spécifier n'importe quel caractère de valeur hexadécimale 0x00 à 0xFF (valeur décimale 0 à 255).

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCU — Le coût de base dépend du type de match que vous utilisez.

- Correspond exactement à la chaîne — 2
- Commence par une chaîne — 2
- Se termine par une ficelle — 2
- Contient une chaîne — 10
- Contient le mot — 10

Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.

Ce type d'instruction fonctionne sur un composant de requête Web et nécessite les paramètres de composant de demande suivants :

- Composant de demande : partie de la requête Web destinée à inspecter, par exemple, une chaîne de requête ou le corps de la requête.

> **Warning**
>
> Si vous inspectez les composants de la requête Body, JSON body, Headers ou Cookies, renseignez-vous sur les limites relatives à Gestion des composants de demande surdimensionnés dans AWS WAF la quantité de contenu AWS WAF pouvant être inspectée.

Pour plus d'informations sur les composants des requêtes Web, consultezSpécification et gestion des composants de requête Web.

- Transformations de texte facultatives : transformations que vous AWS WAF souhaitez effectuer sur le composant de demande avant de l'inspecter. Par exemple, vous pouvez passer en minuscules ou normaliser les espaces blancs. Si vous spécifiez plusieurs transformations, AWS WAF traitez-les dans l'ordre indiqué. Pour plus d'informations, veuillez consulter Options de transformation du texte.

En outre, cette instruction nécessite les paramètres suivants :

- Chaîne à correspondre : il s'agit de la chaîne que vous AWS WAF souhaitez comparer au composant de demande spécifié. Généralement, la chaîne est composée de caractères ASCII affichables, mais vous pouvez spécifier n'importe quel caractère de valeur hexadécimale 0x00 à 0xFF (valeur décimale 0 à 255).
- Condition de correspondance des chaînes : indique le type de recherche que vous AWS WAF souhaitez effectuer.
  - Correspond exactement à la chaîne — La chaîne et la valeur du composant de requête sont identiques.
  - Commence par une chaîne — La chaîne apparaît au début du composant de demande.
  - Se termine par une chaîne — La chaîne apparaît à la fin du composant de demande.
  - Contient une chaîne — La chaîne apparaît n'importe où dans le composant de demande.
  - Contient un mot : la chaîne que vous spécifiez doit apparaître dans le composant de demande.

    Pour cette option, les chaînes que vous spécifiez doivent contenir uniquement des caractères alphanumériques ou un trait de soulignement (A-Z, a-z, 0-9 ou _).

    L'un des éléments suivants doit être vrai pour que la demande corresponde :

- La chaîne correspond exactement à la valeur du composant de demande, telle que la valeur d'un en-tête.
- La chaîne est au début du composant de demande et est suivie par un caractère autre qu'un caractère alphanumérique ou un soulignement (_) : par exemple, `BadBot;`.
- La chaîne est à la fin du composant de demande et est suivie par un caractère autre qu'un caractère alphanumérique ou un soulignement (_) : par exemple, `;BadBot`.
- La chaîne est au milieu du composant de demande et est précédée et suivie de caractères autre que des caractères alphanumériques ou de soulignement (_) : par exemple, `-BadBot;`.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour le type Match, choisissez String match condition, puis renseignez les chaînes que vous souhaitez comparer.
- API — ByteMatchStatement

Instruction d'attaque par scripts inter-site de règle

Une instruction d'attaque XSS (cross-site scripting) détecte la présence de scripts malveillants dans un composant de requête Web. Lors d'une attaque XSS, l'attaquant utilise les vulnérabilités d'un site Web bénin pour injecter des scripts de site client malveillants dans d'autres navigateurs Web légitimes.

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCU — 40 WCU, comme coût de base. Si vous utilisez le composant de requête Tous les paramètres de requête, ajoutez 10 WCU. Si vous utilisez le corps JSON du composant de demande, doublez le coût de base des WCU. Pour chaque transformation de texte que vous appliquez, ajoutez 10 WCU.

Ce type d'instruction fonctionne sur un composant de requête Web et nécessite les paramètres de composant de demande suivants :

- Composant de demande : partie de la requête Web destinée à inspecter, par exemple, une chaîne de requête ou le corps de la requête.

> **Warning**
>
> Si vous inspectez les composants de la requête Body, JSON body, Headers ou Cookies, renseignez-vous sur les limites relatives à Gestion des composants de demande surdimensionnés dans AWS WAF la quantité de contenu AWS WAF pouvant être inspectée.

Pour plus d'informations sur les composants des requêtes Web, consultezSpécification et gestion des composants de requête Web.

- Transformations de texte facultatives : transformations que vous AWS WAF souhaitez effectuer sur le composant de demande avant de l'inspecter. Par exemple, vous pouvez passer en minuscules ou normaliser les espaces blancs. Si vous spécifiez plusieurs transformations, AWS WAF traitez-les dans l'ordre indiqué. Pour plus d'informations, consultez Options de transformation du texte.

Où trouver cette déclaration de règle

- Générateur de règles sur console : pour Type de match, choisissez Attack match condition > Contient des attaques par injection XSS.
- API — XssMatchStatement

Déclarations de règles logiques

Utilisez des instructions de règles logiques pour combiner d'autres instructions ou annuler leurs résultats. Chaque instruction de règle logique prend au moins une instruction imbriquée.

Pour combiner ou annuler de manière logique les résultats des instructions de règle, vous imbriquez les instructions sous des instructions de règles logiques.

Les déclarations de règles logiques sont imbriquables. Vous pouvez les imbriquer dans d'autres instructions de règles logiques et les utiliser dans des instructions de portée réduite. Pour plus d'informations sur les instructions de portée réduite, consultez. Déclarations de portée réduite

> **Note**
>
> L'éditeur visuel de la console prend en charge un niveau d'imbrication des instructions de règle, ce qui fonctionne pour de nombreux besoins. Pour imbriquer davantage de niveaux, modifiez la représentation JSON de la règle sur la console ou utilisez les API.

Ce tableau décrit les instructions de règles logiques et fournit des directives pour calculer l'utilisation des unités de capacité ACL Web (WCU) pour chacune d'entre elles. Pour de plus amples informations sur les WCU, veuillez consulter AWS WAF unités de capacité ACL Web (WCU).

Instruction logique	Description	WCU
Logique AND	Combine des instructions imbriquées avec la AND logique.	Basé sur des instructions imbriquées
Logique NOT	Annule les résultats d'une instruction imbriquée.	Basé sur une instruction imbriquée
Logique OR	Combine des instructions imbriquées avec la OR logique.	Basé sur des instructions imbriquées

ANDdéclaration de règle

L'instruction de AND règle combine des instructions imbriquées avec une AND opération logique, de sorte que toutes les instructions imbriquées doivent correspondre pour que l'ANDinstruction corresponde. Cela nécessite au moins deux instructions imbriquées.

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCus — Cela dépend des instructions imbriquées.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour Si une demande, choisissez correspond à toutes les instructions (ET), puis complétez les instructions imbriquées.

- API — AndStatement

Exemples

La liste suivante montre l'utilisation d'instructions AND de règles NOT logiques pour éliminer les faux positifs des correspondances pour une instruction d'attaque par injection SQL. Pour cet exemple, supposons que nous puissions écrire une instruction de correspondance d'un octet pour répondre aux demandes qui génèrent des faux positifs.

L'instruction AND correspond aux demandes qui ne correspondent pas à l'instruction de correspondance d'octets et qui correspondent à l'instruction d'attaque par injection SQL.

```
{
      "Name": "SQLiExcludeFalsePositives",
      "Priority": 0,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "NotStatement": {
                "Statement": {
                  "ByteMatchStatement": {
                    "SearchString": "string identifying a false positive",
                    "FieldToMatch": {
                      "Body": {
                        "OversizeHandling": "MATCH"
                      }
                    },
                    "TextTransformations": [
                      {
                        "Priority": 0,
                        "Type": "NONE"
                      }
                    ],
                    "PositionalConstraint": "CONTAINS"
                  }
                }
              }
            },
            {
              "SqliMatchStatement": {
                "FieldToMatch": {
```

```
                "Body": {
                  "OversizeHandling": "MATCH"
                }
              },
              "TextTransformations": [
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ]
            }
          }
        ]
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "SQLiExcludeFalsePositives"
    }
  }
```

À l'aide de l'éditeur visuel de règles de console, vous pouvez imbriquer une instruction non logique ou une NOT instruction sous une AND instruction OR or. L'imbrication de l'NOTinstruction est illustrée dans l'exemple précédent.

À l'aide de l'éditeur visuel de règles de console, vous pouvez imbriquer la plupart des instructions imbriquables dans une instruction de règle logique, telle que celle illustrée dans l'exemple précédent. Vous ne pouvez pas utiliser l'éditeur visuel pour imbriquer OR des AND instructions. Pour configurer ce type d'imbrication, vous devez fournir votre déclaration de règle au format JSON. Par exemple, la liste de règles JSON suivante inclut une OR instruction imbriquée dans une AND instruction.

```
{
  "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"
  }
}
```

NOTdéclaration de règle

L'instruction de NOT règle annule logiquement les résultats d'une seule instruction imbriquée, de sorte que les instructions imbriquées ne doivent pas correspondre pour que l'NOTinstruction corresponde, et vice versa. Cela nécessite une instruction imbriquée.

Par exemple, si vous souhaitez bloquer les demandes qui ne proviennent pas d'un pays spécifique, créez une NOT déclaration dont l'action est définie pour bloquer et imbriquez une déclaration de correspondance géographique spécifiant le pays.

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCus — Cela dépend de l'instruction imbriquée.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour Si une demande, choisissez ne correspond pas à l'instruction (NOT), puis renseignez l'instruction imbriquée.
- API — NotStatement

ORdéclaration de règle

L'instruction de OR règle combine des instructions imbriquées avec de OR la logique, de sorte que l'une des instructions imbriquées doit correspondre pour que l'ORinstruction corresponde. Cela nécessite au moins deux instructions imbriquées.

Par exemple, si vous souhaitez bloquer les demandes provenant d'un pays spécifique ou contenant une chaîne de requête spécifique, vous pouvez créer une OR instruction et y imbriquer une

instruction de correspondance géographique pour le pays et une instruction de correspondance de chaîne pour la chaîne de requête.

Si vous souhaitez plutôt bloquer les demandes qui ne proviennent pas d'un pays spécifique ou qui contiennent une chaîne de requête spécifique, vous devez modifier l'ORinstruction précédente pour imbriquer l'instruction de correspondance géographique un niveau plus bas, à l'intérieur d'une NOT instruction. Ce niveau d'imbrication nécessite que vous utilisiez le format JSON, car la console ne prend en charge qu'un seul niveau d'imbrication.

Imbriquable : vous pouvez imbriquer ce type de déclaration.

WCus — Cela dépend des instructions imbriquées.

Où trouver cette déclaration de règle

- Générateur de règles sur la console : pour Si une demande, choisissez correspond à au moins une des instructions (OR), puis renseignez les instructions imbriquées.
- API — OrStatement

Exemples

La liste suivante montre l'utilisation de OR pour combiner deux autres instructions. L'ORinstruction correspond si l'une des instructions imbriquées correspond.

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

À l'aide de l'éditeur visuel de règles de console, vous pouvez imbriquer la plupart des instructions imbriquables dans une instruction de règle logique, mais vous ne pouvez pas utiliser l'éditeur visuel pour imbriquer OR des AND instructions. Pour configurer ce type d'imbrication, vous devez fournir votre déclaration de règle au format JSON. Par exemple, la liste de règles JSON suivante inclut une OR instruction imbriquée dans une AND instruction.

```
{
  "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"
  }
}
```

Instruction de règle basée sur un taux

Une règle basée sur le taux compte les demandes entrantes et limite le débit des demandes lorsqu'elles arrivent trop rapidement. La règle agrège les demandes en fonction de vos critères, et compte et limite le taux des groupements agrégés, en fonction de la fenêtre d'évaluation, de la limite de demandes et des paramètres d'action de la règle.

> **Note**
>
> Vous pouvez également limiter le débit des requêtes Web en utilisant le niveau de protection ciblé du groupe de règles AWS gérées par Bot Control. L'utilisation de ce groupe de règles géré entraîne des frais supplémentaires. Pour plus d'informations, consultez Options de limitation du débit dans les règles basées sur les taux et dans les règles de contrôle des bots ciblées.

AWS WAF suit et gère les requêtes Web séparément pour chaque instance d'une règle basée sur le taux que vous utilisez. Par exemple, si vous fournissez les mêmes paramètres de règle basés sur le taux dans deux ACL Web, chacune des deux instructions de règle représente une instance distincte de la règle basée sur le taux et chacune bénéficie de son propre suivi et de sa propre gestion par. AWS WAF Si vous définissez une règle basée sur les taux au sein d'un groupe de règles, puis que vous utilisez ce groupe de règles à plusieurs endroits, chaque utilisation crée une instance distincte de la règle basée sur les taux qui fait l'objet de son propre suivi et de sa propre gestion. AWS WAF

Non imbriquable : vous ne pouvez pas imbriquer ce type d'instruction dans d'autres instructions. Vous pouvez l'inclure directement dans une ACL Web ou un groupe de règles.

Instruction de portée réduite : ce type de règle peut adopter une instruction de portée réduite, afin de réduire la portée des demandes suivies par la règle et les limites de débit. L'instruction scope-down peut être facultative ou obligatoire, en fonction de vos autres paramètres de configuration des règles. Les détails sont présentés dans cette section. Pour des informations générales sur les instructions de portée réduite, consultez. Déclarations de portée réduite

WCU — 2, comme coût de base. Pour chaque clé d'agrégation personnalisée que vous spécifiez, ajoutez 30 WCU. Si vous utilisez une instruction scope-down dans la règle, calculez et ajoutez les WCU correspondantes.

Où trouver cette déclaration de règle

- Générateur de règles dans votre ACL Web, sur la console : sous Règle, pour Type, choisissez Règle basée sur le taux.
- API — RateBasedStatement

Rubriques

Paramètres de haut niveau des règles basées sur le taux

Une instruction de règle basée sur le taux utilise les paramètres de haut niveau suivants :

- Fenêtre d'évaluation : durée, en secondes, à AWS WAF inclure dans le nombre de demandes, si l'on considère l'heure actuelle. Par exemple, pour un paramètre de 120, lorsque AWS WAF le taux est vérifié, il compte les demandes pendant les 2 minutes précédant immédiatement l'heure actuelle. Les paramètres valides sont 60 (1 minute), 120 (2 minutes), 300 (5 minutes) et 600 (10 minutes), et 300 (5 minutes) est la valeur par défaut.

  Ce paramètre ne détermine pas la fréquence AWS WAF à laquelle le taux est vérifié, mais la distance parcourue à chaque vérification. AWS WAF vérifie le taux fréquemment, avec un calendrier indépendant du réglage de la fenêtre d'évaluation.
- Limite de taux : nombre maximum de demandes correspondant à vos critères qui AWS WAF doivent être suivies pendant la période d'évaluation spécifiée. La limite minimale autorisée est de 100. Lorsque cette limite est dépassée, AWS WAF applique le paramètre d'action de la règle aux demandes supplémentaires correspondant à vos critères.

  AWS WAF applique une limite de débit proche de la limite que vous avez définie, mais ne garantit pas une correspondance exacte entre les limites. Pour plus d'informations, consultez Mises en garde relatives aux règles basées sur les taux.

- Agrégation des demandes : les critères d'agrégation à utiliser sur le Web demandent que la règle basée sur le taux compte et limite le débit. La limite de débit que vous définissez s'applique à chaque instance d'agrégation. Pour plus d'informations, consultez Options et clés d'agrégation et Instances d'agrégation et nombres.
- Action : action à effectuer en réponse aux demandes dont le taux est limité par la règle. Vous pouvez utiliser n'importe quelle action de règle, saufAllow. Ceci est défini au niveau de la règle, comme d'habitude, mais comporte certaines restrictions et certains comportements spécifiques aux règles basées sur les taux. Pour des informations générales sur les actions relatives aux règles, consultezAction de la règle. Pour des informations spécifiques à la limitation du débit, consultez Comportement limitant le débit des demandes de règles basées sur le taux cette section.
- Étendue de l'inspection et limitation du débit : vous pouvez réduire la portée des demandes suivies par le relevé basé sur les taux et les limites de taux en ajoutant un relevé de portée inférieure. Si vous spécifiez une instruction scope-down, la règle agrège, compte et limite le débit uniquement les demandes qui correspondent à l'instruction scope-down. Si vous choisissez l'option d'agrégation des demandes Count all, l'instruction scope-down est requise. Pour plus d'informations sur les instructions de portée réduite, consultez. Déclarations de portée réduite
- (Facultatif) Configuration IP transférée : elle n'est utilisée que si vous spécifiez l'adresse IP dans l'en-tête de votre agrégation de demandes, soit seule, soit dans le cadre des paramètres de clés personnalisés. AWS WAF récupère la première adresse IP dans l'en-tête spécifié et l'utilise comme valeur d'agrégation. Un en-tête courant est utilisé à cette fin`X-Forwarded-For`, mais vous pouvez spécifier n'importe quel en-tête. Pour plus d'informations, voir Adresse IP transférée.

Mises en garde relatives aux règles basées sur les taux

AWS WAF la limitation du débit est conçue pour contrôler les taux de demandes élevés et protéger la disponibilité de votre application de la manière la plus efficace possible. Il n'est pas destiné à une limitation précise du taux de demandes.

- AWS WAF estime le taux de demandes actuel à l'aide d'un algorithme qui accorde plus d'importance aux demandes les plus récentes. Pour cette raison, AWS WAF appliquera une limite de taux proche de la limite que vous avez définie, mais cela ne garantit pas une correspondance exacte entre les limites.
- Chaque fois que le taux de demandes est AWS WAF estimé, AWS WAF il revient sur le nombre de demandes reçues pendant la fenêtre d'évaluation configurée. En raison de cela et d'autres facteurs tels que les délais de propagation, il est possible que les demandes arrivent à un rythme trop élevé pendant plusieurs minutes avant de les AWS WAF détecter et de les limiter. De même, le taux de

demandes peut être inférieur à la limite pendant un certain temps avant de AWS WAF détecter la diminution et d'interrompre l'action de limitation du débit. Ce délai est généralement inférieur à 30 secondes.

- Si vous modifiez l'un des paramètres de limite de débit d'une règle en cours d'utilisation, la modification réinitialise le nombre de limites de débit de la règle. Cela peut suspendre les activités de limitation de débit prévues par la règle pendant une minute au maximum. Les paramètres de limite de débit sont la fenêtre d'évaluation, la limite de débit, les paramètres d'agrégation des demandes, la configuration IP transférée et l'étendue de l'inspection.

Options et clés d'agrégation de règles basées sur le taux

Par défaut, une règle basée sur le débit agrège et limite les demandes en fonction de l'adresse IP de la demande. Vous pouvez configurer la règle pour utiliser diverses autres clés d'agrégation et combinaisons de touches. Par exemple, vous pouvez agréger en fonction d'une adresse IP transférée, de la méthode HTTP ou d'un argument de requête. Vous pouvez également spécifier des combinaisons de clés d'agrégation, telles que l'adresse IP et la méthode HTTP, ou les valeurs de deux cookies différents.

> **Note**
>
> Tous les composants de demande que vous spécifiez dans la clé d'agrégation doivent être présents dans une requête Web pour que la demande soit évaluée ou que le taux soit limité par la règle.

Vous pouvez configurer votre règle basée sur le taux avec les options d'agrégation suivantes.

- Adresse IP source : agrégée en utilisant uniquement l'adresse IP de l'origine de la requête Web.

  L'adresse IP source peut ne pas contenir l'adresse du client d'origine. Si une requête Web passe par un ou plusieurs proxys ou équilibreurs de charge, celle-ci contiendra l'adresse du dernier proxy.
- Adresse IP dans l'en-tête : agrégation en utilisant uniquement une adresse client dans un en-tête HTTP. Cette adresse est également appelée adresse IP transférée.

  Avec cette configuration, vous spécifiez également un comportement de secours à appliquer à une requête Web dont l'en-tête contient une adresse IP mal formée. Le comportement de remplacement définit le résultat correspondant à la demande, qu'il corresponde ou non. En cas d'absence de correspondance, la règle basée sur le taux ne compte pas ou ne limite pas le taux

de la demande. Pour la correspondance, la règle basée sur le taux regroupe la demande avec les autres demandes dont l'adresse IP est mal formée dans l'en-tête spécifié.

Soyez prudent avec cette option, car les en-têtes peuvent être gérés de manière incohérente par les proxys et ils peuvent également être modifiés pour contourner l'inspection. Pour plus d'informations et les meilleures pratiques, consultezAdresse IP transférée.

- Tout compter : comptez et limitez le débit de toutes les demandes qui correspondent à l'énoncé de portée réduite de la règle. Cette option nécessite une instruction scope-down. Ceci est généralement utilisé pour limiter le débit d'un ensemble spécifique de demandes, telles que toutes les demandes portant une étiquette spécifique ou toutes les demandes provenant d'une zone géographique spécifique.
- Clés personnalisées : agrégation à l'aide d'une ou de plusieurs clés d'agrégation personnalisées. Pour combiner l'une des options d'adresse IP avec d'autres clés d'agrégation, définissez-les ici sous Clés personnalisées.

  Les clés d'agrégation personnalisées sont un sous-ensemble des options des composants de demande Web décrites surOptions de composants de demande.

  Les principales options sont les suivantes. Sauf indication contraire, vous pouvez utiliser une option plusieurs fois, par exemple deux en-têtes ou trois espaces de noms d'étiquettes.

  - Espace de noms d'étiquettes : utilisez un espace de noms d'étiquettes comme clé d'agrégation. Chaque nom d'étiquette complet distinct qui possède l'espace de noms d'étiquette spécifié contribue à l'instance d'agrégation. Si vous utilisez un seul espace de noms d'étiquette comme clé personnalisée, chaque nom d'étiquette définit entièrement une instance d'agrégation.

    La règle basée sur le taux utilise uniquement les étiquettes qui ont été ajoutées à la demande par des règles préalablement évaluées dans l'ACL Web.

    Pour plus d'informations sur les espaces de noms et les noms d'étiquettes, consultezAWS WAF syntaxe des étiquettes et exigences de dénomination.
  - En-tête : utilisez un en-tête nommé comme clé d'agrégation. Chaque valeur distincte de l'en-tête contribue à l'instance d'agrégation.

    L'en-tête nécessite une transformation de texte facultative. veuillez consulter Options de transformation du texte.
  - Cookie : utilisez un cookie nommé comme clé d'agrégation. Chaque valeur distincte du cookie contribue à l'instance d'agrégation.

Le cookie effectue une transformation de texte facultative. veuillez consulter Options de transformation du texte.

- Argument de requête : utilisez un seul argument de requête dans la demande comme clé d'agrégation. Chaque valeur distincte pour l'argument de requête nommé contribue à l'instance d'agrégation.

  L'argument Query accepte une transformation de texte facultative. veuillez consulter Options de transformation du texte.

- Chaîne de requête : utilisez l'intégralité de la chaîne de requête de la demande comme clé agrégée. Chaque chaîne de requête distincte contribue à l'instance d'agrégation. Vous ne pouvez utiliser ce type de clé qu'une seule fois.

  La chaîne de requête accepte une transformation de texte facultative. veuillez consulter Options de transformation du texte.

- Chemin de l'URI — Utilisez le chemin de l'URI dans la demande comme clé agrégée. Chaque chemin d'URI distinct contribue à l'instance d'agrégation. Vous ne pouvez utiliser ce type de clé qu'une seule fois.

  Le chemin de l'URI effectue une transformation de texte facultative. veuillez consulter Options de transformation du texte.

- Méthode HTTP : utilisez la méthode HTTP de la demande comme clé d'agrégation. Chaque méthode HTTP distincte contribue à l'instance d'agrégation. Vous ne pouvez utiliser ce type de clé qu'une seule fois.

- Adresse IP : agrégation à l'aide de l'adresse IP provenant de l'origine de la demande Web en combinaison avec d'autres clés.

  Il se peut qu'il ne contienne pas l'adresse du client d'origine. Si une requête Web passe par un ou plusieurs proxys ou équilibreurs de charge, celle-ci contiendra l'adresse du dernier proxy.

- Adresse IP dans l'en-tête — Agrégez en utilisant l'adresse du client dans un en-tête HTTP en combinaison avec d'autres clés. Cette adresse est également appelée adresse IP transférée.

  Soyez prudent avec cette option, car les en-têtes peuvent être gérés de manière incohérente par les proxys et ils peuvent être modifiés pour contourner l'inspection. Pour plus d'informations et les meilleures pratiques, consultezAdresse IP transférée.

Instances et nombres d'agrégation de règles basés sur le taux

Lorsqu'une règle basée sur le taux évalue les requêtes Web à l'aide de vos critères d'agrégation, chaque ensemble unique de valeurs trouvé par la règle pour les clés d'agrégation spécifiées définit une instance d'agrégation unique.

- Clés multiples : si vous avez défini plusieurs clés personnalisées, la valeur de chaque clé contribue à la définition de l'instance d'agrégation. Chaque combinaison unique de valeurs définit une instance d'agrégation.
- Clé unique : si vous avez choisi une seule clé, soit dans les clés personnalisées, soit en sélectionnant l'une des adresses IP singleton, chaque valeur unique de la clé définit une instance d'agrégation.
- Tout compter, aucune clé : si vous avez sélectionné l'option d'agrégation Tout compter, toutes les demandes évaluées par la règle appartiennent à une seule instance d'agrégation pour la règle. Ce choix nécessite une instruction scope-down.

Une règle basée sur le taux compte les requêtes Web séparément pour chaque instance d'agrégation qu'elle identifie.

Supposons, par exemple, qu'une règle basée sur le débit évalue les requêtes Web avec l'adresse IP et les valeurs de méthode HTTP suivantes :

- Adresse IP 10.1.1.1, méthode HTTP POST
- Adresse IP 10.1.1.1, méthode HTTP GET
- Adresse IP 127.0.0.0, méthode HTTP POST
- Adresse IP 10.1.1.1, méthode HTTP GET

La règle crée différentes instances d'agrégation en fonction de vos critères d'agrégation.

- Si le critère d'agrégation est uniquement l'adresse IP, chaque adresse IP individuelle est une instance d'agrégation et AWS WAF compte les demandes séparément pour chacune d'entre elles. Les instances d'agrégation et le nombre de demandes dans notre exemple seraient les suivants :
  - Adresse IP 10.1.1.1 : compte 3
  - Adresse IP 127.0.0.0 : compte 1

- Si le critère d'agrégation est la méthode HTTP, chaque méthode HTTP individuelle est une instance d'agrégation. Les instances d'agrégation et le nombre de demandes dans notre exemple seraient les suivants :
  - Méthode HTTP POST : compte 2
  - Méthode HTTP GET : count 2
- Si les critères d'agrégation sont l'adresse IP et la méthode HTTP, chaque adresse IP et chaque méthode HTTP contribueront à l'instance d'agrégation combinée. Les instances d'agrégation et le nombre de demandes dans notre exemple seraient les suivants :
  - Adresse IP 10.1.1.1, méthode HTTP POST : compte 1
  - Adresse IP 10.1.1.1, méthode HTTP GET : count 2
  - Adresse IP 127.0.0.0, méthode HTTP POST : compte 1

Comportement limitant le débit des demandes de règles basées sur le taux

Les critères AWS WAF utilisés pour limiter le débit des demandes pour une règle basée sur le taux sont les mêmes que ceux AWS WAF utilisés pour agréger les demandes relatives à la règle. Si vous définissez une instruction de portée réduite pour la règle, AWS WAF seuls les agrégats, les dénombrements et les demandes de limite de débit correspondent à l'instruction de portée réduite.

Les critères de correspondance qui amènent une règle basée sur le taux à appliquer ses paramètres d'action de règle à une requête Web spécifique sont les suivants :

- La requête Web correspond à l'instruction scope-down de la règle, si une telle instruction est définie.
- La requête Web appartient à une instance d'agrégation dont le nombre de demandes est actuellement supérieur à la limite fixée par la règle.

Comment AWS WAF s'applique l'action de la règle

Lorsqu'une règle basée sur le taux applique une limitation de débit à une demande, elle applique l'action de la règle et, si vous avez défini un traitement ou un étiquetage personnalisé dans votre spécification d'action, la règle les applique. Cette gestion des demandes est identique à la manière dont une règle de correspondance applique ses paramètres d'action aux requêtes Web correspondantes. Une règle basée sur le taux applique uniquement des libellés ou exécute d'autres actions sur les demandes pour lesquelles elle limite activement le débit.

Vous pouvez utiliser n'importe quelle action de règle, à l'exception deAllow. Pour des informations générales sur les actions relatives aux règles, consultezAction de la règle.

La liste suivante décrit le fonctionnement de la limitation de débit pour chacune des actions.

- Block— AWS WAF bloque la demande et applique tout comportement de blocage personnalisé que vous avez défini.
- Count— AWS WAF compte la demande, applique les en-têtes ou étiquettes personnalisés que vous avez définis et poursuit l'évaluation ACL Web de la demande.

  Cette action ne limite pas le nombre de demandes. Il ne compte que les demandes qui dépassent la limite.
- CAPTCHAor Challenge — AWS WAF gère la demande comme a Block ou comme aCount, selon l'état du jeton de la demande.

  Cette action ne limite pas le nombre de demandes contenant des jetons valides. Cela limite le taux de demandes dépassant la limite et pour lesquelles il manque également des jetons valides.

  - Si la demande ne contient pas de jeton valide et non expiré, l'action bloque la demande et renvoie le casse-tête CAPTCHA ou le défi du navigateur au client.

    Si l'utilisateur final ou le navigateur du client répond correctement, le client reçoit un jeton valide et renvoie automatiquement la demande initiale. Si la limitation du débit pour l'instance d'agrégation est toujours en vigueur, l'action sera appliquée à cette nouvelle demande contenant le jeton valide et non expiré, comme décrit dans le point suivant de la bullet.
  - Si la demande contient un jeton valide et non expiré, l'Challengeaction CAPTCHA ou vérifie le jeton et n'entreprend aucune action sur la demande, de la même manière que l'Countaction. La règle basée sur le taux renvoie l'évaluation de la demande à l'ACL Web sans prendre aucune mesure d'arrêt, et l'ACL Web poursuit son évaluation de la demande.

  Pour plus d’informations, consultez CAPTCHAet Challenge dans AWS WAF.

Si vous limitez le débit uniquement à l'adresse IP ou à l'adresse IP transférée

Lorsque vous configurez la règle pour limiter uniquement l'adresse IP pour l'adresse IP transférée, l'instance de règle peut limiter le débit jusqu'à 10 000 adresses IP. Si une instance de règle identifie plus de 10 000 adresses IP à limiter, elle limite uniquement les 10 000 plus grands expéditeurs.

Avec cette configuration, vous pouvez récupérer la liste des adresses IP pour lesquelles une règle basée sur le débit limite actuellement le débit. Si vous utilisez une instruction scope-down, les demandes dont le débit est limité sont uniquement celles de la liste d'adresses IP qui correspondent à l'instruction scope-down. Pour plus d'informations sur la récupération de la liste d'adresses IP, consultezRépertorier les adresses IP dont le débit est limité par des règles basées sur le débit.

Exemples de règles basées sur les taux

Cette section décrit des exemples de configuration pour divers cas d'utilisation courants de règles basées sur les taux.

Chaque exemple fournit une description du cas d'utilisation, puis montre la solution dans les listes JSON pour les règles configurées personnalisées.

> **Note**
>
> Les listes JSON présentées dans ces exemples ont été créées dans la console en configurant la règle, puis en la modifiant à l'aide de l'éditeur Rule JSON.

Rubriques

- Limiter le débit des demandes à une page de connexion
- Débit : limite les demandes adressées à une page de connexion à partir de n'importe quelle adresse IP ou paire d'agents utilisateurs
- Limite de débit les demandes pour lesquelles il manque un en-tête spécifique
- Débit : limitez les demandes avec des étiquettes spécifiques
- Limite de débit les demandes d'étiquettes ayant un espace de noms d'étiquette spécifié

Limiter le débit des demandes à une page de connexion

Pour limiter le nombre de demandes adressées à la page de connexion de votre site Web sans affecter le trafic vers le reste de votre site, vous pouvez créer une règle basée sur le taux avec une instruction de délimitation qui fait correspondre les demandes à votre page de connexion et avec l'agrégation des demandes définie sur Tout compter.

La règle basée sur le taux comptera toutes les demandes pour la page de connexion dans une seule instance d'agrégation et appliquera l'action de la règle lorsque les demandes dépassent la limite.

La liste JSON suivante montre un exemple de cette configuration de règle. L'option d'agrégation Count All est répertoriée dans le JSON en tant que paramètre`CONSTANT`. Cet exemple correspond aux pages de connexion qui commencent par`/login`.

```
{
  "Name": "test-rbr",
  "Priority": 0,
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-rbr"
  },
  "Statement": {
    "RateBasedStatement": {
      "Limit": 1000,
      "EvaluationWindowSec": 300,
      "AggregateKeyType": "CONSTANT",
      "ScopeDownStatement": {
        "ByteMatchStatement": {
          "FieldToMatch": {
            "UriPath": {}
          },
          "PositionalConstraint": "STARTS_WITH",
          "SearchString": "/login",
          "TextTransformations": [
            {
              "Type": "NONE",
              "Priority": 0
            }
          ]
        }
      }
    }
  }
}
```

Débit : limite les demandes adressées à une page de connexion à partir de n'importe quelle adresse IP ou paire d'agents utilisateurs

Pour limiter le nombre de demandes d'adresse IP adressées à la page de connexion de votre site Web, définissez les paires d'agents utilisateurs qui dépassent votre limite, définissez l'agrégation des demandes sur Clés personnalisées et fournissez les critères d'agrégation.

La liste JSON suivante montre un exemple de cette configuration de règle. Dans cet exemple, nous avons fixé la limite à 100 demandes par période de cinq minutes par adresse IP, paire d'agents utilisateurs.

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

Limite de débit les demandes pour lesquelles il manque un en-tête spécifique

Pour limiter le nombre de demandes auxquelles il manque un en-tête spécifique, vous pouvez utiliser l'option d'agrégation Count all avec une instruction scope-down. Configurez l'instruction scope-down avec une NOT instruction logique contenant une instruction qui renvoie true uniquement si l'en-tête existe et possède une valeur.

La liste JSON suivante montre un exemple de cette configuration de règle.

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

Débit : limitez les demandes avec des étiquettes spécifiques

Vous pouvez combiner la limitation de débit avec n'importe quelle règle ou groupe de règles qui ajoute des étiquettes aux demandes, afin de limiter le nombre de demandes de différentes catégories. Pour ce faire, configurez votre ACL Web comme suit :

- Ajoutez les règles ou les groupes de règles qui ajoutent des étiquettes, et configurez-les de manière à ce qu'ils ne bloquent pas ou n'autorisent pas les demandes pour lesquelles vous souhaitez limiter le débit. Si vous utilisez des groupes de règles gérés, vous devrez peut-être annuler certaines actions des règles des groupes de règles Count pour obtenir ce comportement.
- Ajoutez une règle basée sur le taux à votre ACL Web avec un paramètre de numéro de priorité supérieur aux règles d'étiquetage et aux groupes de règles. AWS WAF évalue les règles par ordre numérique, en commençant par le plus bas, afin que votre règle basée sur les taux soit exécutée après les règles d'étiquetage. Configurez votre limite de débit sur les étiquettes en combinant

la correspondance des étiquettes dans l'énoncé de portée réduite de la règle et l'agrégation d'étiquettes.

L'exemple suivant utilise le groupe de règles AWS Managed Rules de la liste de réputation Amazon IP. La règle du groupe de règles `AWSManagedIPDDoSList` détecte et étiquette les demandes dont les adresses IP sont connues pour participer activement à des activités DDoS. L'action de la règle est configurée Count dans la définition du groupe de règles. Pour plus d'informations sur le groupe de règles, consultezthe section called “Liste de réputation des adresses IP Amazon”.

La liste JSON ACL Web suivante utilise le groupe de règles de réputation IP suivi d'une règle basée sur le taux de correspondance des étiquettes. La règle basée sur le taux utilise une instruction scope-down pour filtrer les demandes qui ont été marquées par la règle du groupe de règles. L'énoncé de règle basé sur le taux agrège et limite le débit des demandes filtrées en fonction de leur adresse IP.

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesAmazonIpReputationList",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesAmazonIpReputationList"
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesAmazonIpReputationList"
      }
    },
```

```
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 100,
          "EvaluationWindowSec": 300,
          "AggregateKeyType": "IP",
          "ScopeDownStatement": {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:amazon-ip-list:AWSManagedIPDDoSList"
            }
          }
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 28,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

Limite de débit les demandes d'étiquettes ayant un espace de noms d'étiquette spécifié

Les règles de niveau commun du groupe de règles gérées par Bot Control ajoutent des étiquettes pour les robots de différentes catégories, mais elles bloquent uniquement les demandes provenant de robots non vérifiés. Pour plus d'informations sur ces règles, consultezListe des règles de contrôle des bots.

Si vous utilisez le groupe de règles géré par Bot Control, vous pouvez ajouter une limite de débit pour les demandes provenant de robots individuels vérifiés. Pour ce faire, vous ajoutez une règle basée sur le taux qui s'exécute après le groupe de règles Bot Control et agrège les demandes en fonction de leurs étiquettes de nom de bot. Vous spécifiez la clé d'agrégation de l'espace de noms Label et définissez la clé d'espace de noms sur. `awswaf:managed:aws:bot-control:bot:name:` Chaque étiquette unique avec l'espace de noms spécifié définira une instance d'agrégation. Par exemple, les étiquettes `awswaf:managed:aws:bot-control:bot:name:axios` et `awswaf:managed:aws:bot-control:bot:name:curl` chacune définissent une instance d'agrégation.

La liste JSON ACL Web suivante montre cette configuration. La règle décrite dans cet exemple limite les demandes pour une instance d'agrégation de robots uniques à 1 000 sur une période de deux minutes.

```
{
  "Name": "test-web-acl",
  "Id": ...
  "ARN": ...
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesBotControlRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesBotControlRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesBotControlRuleSet": {
                "InspectionLevel": "COMMON"
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
```

```
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesBotControlRuleSet"
      }
    },
    {
      "Name": "test-rbr",
      "Priority": 1,
      "Statement": {
        "RateBasedStatement": {
          "Limit": 1000,
          "EvaluationWindowSec": 120,
          "AggregateKeyType": "CUSTOM_KEYS",
          "CustomKeys": [
            {
              "LabelNamespace": {
                "Namespace": "awswaf:managed:aws:bot-control:bot:name:"
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "test-rbr"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "test-web-acl"
  },
  "Capacity": 82,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:0000000000:webacl:test-web-acl:"
}
```

Répertorier les adresses IP dont le débit est limité par des règles basées sur le débit

Si votre règle basée sur le taux ne s'agrège que sur l'adresse IP ou l'adresse IP transférée, vous pouvez récupérer la liste des adresses IP pour lesquelles la règle limite actuellement le débit. AWS WAF stocke ces adresses IP dans la liste des clés gérées de la règle.

> **Note**
>
> Cette option n'est disponible que si vous regroupez uniquement l'adresse IP ou uniquement une adresse IP dans un en-tête. Si vous utilisez l'agrégation de demandes de clés personnalisées, vous ne pouvez pas récupérer une liste d'adresses IP à débit limité, même si vous utilisez l'une des spécifications d'adresse IP dans vos clés personnalisées.

Une règle basée sur le taux applique son action aux demandes de la liste des clés gérées de la règle qui correspondent à l'instruction scope-down de la règle. Lorsqu'une règle ne comporte aucune instruction de portée réduite, elle applique l'action à toutes les demandes provenant des adresses IP figurant dans la liste. L'action de règle est Block par défaut, mais il peut s'agir de n'importe quelle action de règle valide, à l'exception deAllow. Le nombre maximum d'adresses IP AWS WAF pouvant limiter le débit à l'aide d'une seule instance de règle basée sur le débit est de 10 000. Si plus de 10 000 adresses dépassent la limite de débit, AWS WAF limite celles présentant les taux les plus élevés.

Vous pouvez accéder à la liste des clés gérées d'une règle basée sur le taux à l'aide de la CLI, de l'API ou de l'un des SDK. Cette rubrique couvre l'accès à l'aide de l'interface de ligne de commande et des API. La console ne permet pas d'accéder à la liste pour le moment.

Pour l' AWS WAF API, la commande est GetRateBasedStatementManagedKeys.

Pour la AWS WAF CLI, la commande est get-rate-based-statement-managed-keys.

Ce qui suit montre la syntaxe permettant de récupérer la liste des adresses IP à débit limité pour une règle basée sur le débit utilisée dans une ACL Web sur une distribution Amazon CloudFront .

```
aws wafv2 get-rate-based-statement-managed-keys --scope=CLOUDFRONT --region=us-east-1
 --web-acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

Voici la syntaxe d'une application régionale, d'une API REST Amazon API Gateway, d'un Application Load Balancer, d'une API AWS AppSync GraphQL, d'un groupe d'utilisateurs Amazon Cognito, d'un AWS App Runner service ou d'une instance Verified Access. AWS

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-name=RuleName
```

AWS WAF surveille les requêtes Web et gère les clés indépendamment pour chaque combinaison unique d'ACL Web, de groupe de règles facultatif et de règle basée sur le taux. Par exemple, si vous définissez une règle basée sur le taux au sein d'un groupe de règles, puis que vous utilisez le groupe de règles dans une ACL Web, AWS WAF vous surveillez les requêtes Web et gérez les clés pour cette ACL Web, la déclaration de référence du groupe de règles et l'instance de règle basée sur le taux. Si vous utilisez le même groupe de règles dans une deuxième ACL Web, vous AWS WAF surveillez les requêtes Web et gérez les clés pour cette deuxième utilisation de manière totalement indépendante de la première.

Pour une règle basée sur le taux que vous avez définie au sein d'un groupe de règles, vous devez fournir le nom de la déclaration de référence du groupe de règles dans votre demande, en plus du nom de l'ACL Web et du nom de la règle basée sur le taux au sein du groupe de règles. Ce qui suit montre la syntaxe d'une application régionale dans laquelle la règle basée sur le taux est définie au sein d'un groupe de règles, et le groupe de règles est utilisé dans une ACL Web.

```
aws wafv2 get-rate-based-statement-managed-keys --scope=REGIONAL --region=region --web-
acl-name=WebACLName --web-acl-id=WebACLId --rule-group-rule-name=RuleGroupRuleName --
rule-name=RuleName
```

Déclarations de règles relatives aux groupes de règles

Les déclarations de règles relatives aux groupes de règles ne sont pas imbriquables.

Cette section décrit les instructions de règles de groupe de règles que vous pouvez utiliser dans votre ACL Web. Les unités de capacité ACL Web (WCU) du groupe de règles sont définies par le propriétaire du groupe de règles au moment de sa création. Pour de plus amples informations sur les WCU, veuillez consulter AWS WAF unités de capacité ACL Web (WCU).

Instruction de groupe de règles	Description	WCU
Groupe de règles géré	Exécute les règles définies dans le groupe de règles gérées spécifié.	Défini par le groupe de règles, plus toutes les WCU

Instruction de groupe de règles	Description	WCU
	Vous pouvez réduire la portée des demandes évaluées par le groupe de règles en ajoutant une instruction scope-down. Vous ne pouvez pas imbriquer une instruction de groupe de règles géré dans un autre type d'instruction.	supplémentaires pour une instruction scope-down.
Groupe de règles	Exécute les règles définies dans un groupe de règles que vous gérez. Vous ne pouvez pas ajouter d'instruction de portée réduite à une déclaration de référence de groupe de règles pour votre propre groupe de règles. Vous ne pouvez pas imbriquer une instruction de groupe de règles dans un autre type d'instruction	Vous définissez la limite WCU pour le groupe de règles lorsque vous le créez.

Instruction de groupe de règles géré

L'instruction de règle de groupe de règles gérées ajoute une référence dans la liste de règles de votre ACL web à un groupe de règles gérées. Vous ne voyez pas cette option sous vos instructions de règle sur la console, mais lorsque vous travaillez avec le format JSON de votre liste ACL web, tous les groupes de règles gérés que vous avez ajoutés apparaissent sous les règles ACL Web comme ce type.

Un groupe de règles géré est soit un groupe de règles AWS gérées, dont la plupart sont gratuites pour les AWS WAF clients, soit un groupe de règles AWS Marketplace géré. Vous vous abonnez

automatiquement aux groupes de règles AWS Managed Rules payants lorsque vous les ajoutez à votre ACL Web. Vous pouvez vous abonner à des groupes de règles AWS Marketplace gérés via AWS Marketplace. Pour plus d'informations, consultez Groupes de règles gérés.

Lorsque vous ajoutez un groupe de règles à une ACL Web, vous pouvez remplacer les actions des règles du groupe par Count ou par une autre action de règle. Pour plus d'informations, consultez Options de dérogation aux actions pour les groupes de règles.

Vous pouvez réduire la portée des demandes AWS WAF évaluées à l'aide du groupe de règles. Pour ce faire, vous devez ajouter une instruction scope-down dans l'instruction du groupe de règles. Pour plus d'informations sur les instructions de portée réduite, consultez. Déclarations de portée réduite Cela peut vous aider à gérer la manière dont le groupe de règles affecte votre trafic et à contenir les coûts associés au volume de trafic lorsque vous utilisez le groupe de règles. Pour obtenir des informations et des exemples d'utilisation des instructions de portée réduite avec le groupe de règles géré par AWS WAF Bot Control, consultez. AWS WAF Contrôle des robots

Non imbriquable : vous ne pouvez pas imbriquer ce type d'instruction dans d'autres instructions, ni l'inclure dans un groupe de règles. Vous pouvez l'inclure directement dans une liste ACL web.

(Facultatif) Instruction de portée réduite : ce type de règle utilise une instruction de portée réduite facultative, afin de réduire la portée des demandes évaluées par le groupe de règles. Pour plus d'informations, consultez Déclarations de portée réduite.

WCU — Défini pour le groupe de règles lors de sa création.

Où trouver cette déclaration de règle

- Console — Au cours du processus de création d'une ACL Web, sur la page Ajouter des règles et des groupes de règles, choisissez Ajouter des groupes de règles gérés, puis recherchez et sélectionnez le groupe de règles que vous souhaitez utiliser.
- API — ManagedRuleGroupStatement

Instruction de groupe de règles

L'instruction de règle de groupe de règles ajoute la référence à votre liste de règles ACL web à un groupe de règles que vous gérez. Vous ne voyez pas cette option sous vos instructions de règles sur la console, mais lorsque vous travaillez avec le format JSON de votre liste ACL web, l'un de vos propres groupes de règles que vous avez ajoutés apparaît sous les règles ACL web comme ce type.

Pour de plus amples informations sur l'utilisation de vos propres groupes de règles, reportez-vous à la section Gestion de vos propres groupes de règles.

Lorsque vous ajoutez un groupe de règles à une ACL Web, vous pouvez remplacer les actions des règles du groupe par Count ou par une autre action de règle. Pour plus d'informations, consultez Options de dérogation aux actions pour les groupes de règles.

Non imbriquable : vous ne pouvez pas imbriquer ce type d'instruction dans d'autres instructions, ni l'inclure dans un groupe de règles. Vous pouvez l'inclure directement dans une liste ACL web.

WCU — Défini pour le groupe de règles lors de sa création.

Où trouver cette déclaration de règle

- Console — Au cours du processus de création d'une ACL Web, sur la page Ajouter des règles et des groupes de règles, choisissez Ajouter mes propres règles et groupes de règles, Groupe de règles, puis ajoutez le groupe de règles que vous souhaitez utiliser.
- API — RuleGroupReferenceStatement

Gestion des composants de demande surdimensionnés dans AWS WAF

AWS WAF ne prend pas en charge l'inspection de contenus très volumineux pour le corps des composants de la requête Web, les en-têtes ou les cookies. Le service hôte sous-jacent est soumis à des limites de nombre et de taille pour ce qu'il transmet à AWS WAF des fins d'inspection. Par exemple, le service hôte n'envoie pas plus de 200 en-têtes à. Par conséquent AWS WAF, pour une requête Web contenant 205 en-têtes, AWS WAF vous ne pouvez pas inspecter les 5 derniers en-têtes.

Lorsque AWS WAF vous autorisez une requête Web à accéder à votre ressource protégée, l'intégralité de la demande Web est envoyée, y compris tout contenu dépassant les limites de nombre et de taille qui ont AWS WAF pu être inspectées.

Limites de taille pour l'inspection des composants

Les limites de taille d'inspection des composants sont les suivantes :

- **`Body`**et **`JSON Body`** — Pour Application Load Balancer et AWS AppSync, AWS WAF peut inspecter les 8 premiers Ko du corps d'une demande. Par défaut CloudFront, API Gateway,

Amazon Cognito, App Runner et Verified Access AWS WAF peuvent inspecter les 16 premiers Ko, et vous pouvez augmenter la limite jusqu'à 64 Ko dans votre configuration ACL Web. Pour plus d'informations, consultez Gestion des limites de taille des organismes inspectés.

- **`Headers`**— AWS WAF peut inspecter au maximum les 8 premiers Ko (8 192 octets) des en-têtes de requête et au plus les 200 premiers en-têtes. Le contenu peut être consulté AWS WAF jusqu'à la première limite atteinte.
- **`Cookies`**— AWS WAF peut inspecter au maximum les 8 premiers Ko (8 192 octets) des cookies de demande et au plus les 200 premiers cookies. Le contenu peut être consulté AWS WAF jusqu'à la première limite atteinte.

Options de gestion surdimensionnées pour vos déclarations de règles

Lorsque vous rédigez une instruction de règle qui inspecte l'un de ces types de composants de demande, vous spécifiez comment gérer les composants surdimensionnés. La gestion des surdimensionnements indique AWS WAF ce qu'il faut faire avec une requête Web lorsque le composant de demande inspecté par la règle dépasse les limites de taille.

Les options de gestion des composants surdimensionnés sont les suivantes :

- Continue— Inspectez le composant de demande normalement conformément aux critères d'inspection des règles. AWS WAF inspectera le contenu du composant de la demande qui respecte les limites de taille.
- Match— Traitez la requête Web comme correspondant à l'énoncé de règle. AWS WAF applique l'action de règle à la demande sans l'évaluer par rapport aux critères d'inspection de la règle.
- No match— Traitez la requête Web comme ne correspondant pas à l'énoncé de règle sans l'évaluer par rapport aux critères d'inspection de la règle. AWS WAF poursuit son inspection de la requête Web en utilisant le reste des règles de l'ACL Web comme il le ferait pour toute règle non correspondante.

Dans la AWS WAF console, vous devez choisir l'une de ces options de gestion. En dehors de la console, l'option par défaut estContinue.

Si vous utilisez cette Match option dans une règle dont l'action est définie surBlock, la règle bloquera une demande dont le composant inspecté est surdimensionné. Quelle que soit la configuration, la disposition finale de la demande dépend de divers facteurs, tels que la configuration des autres règles de votre ACL Web et le paramètre d'action par défaut de l'ACL Web.

Gestion des surdimensionnements dans des groupes de règles dont vous n'êtes pas le propriétaire

Les limites de taille et de nombre de composants s'appliquent à toutes les règles que vous utilisez dans votre ACL Web. Cela inclut toutes les règles que vous utilisez mais que vous ne gérez pas, dans les groupes de règles gérés et dans les groupes de règles partagés avec vous par un autre compte.

Lorsque vous utilisez un groupe de règles que vous ne gérez pas, celui-ci peut comporter une règle qui inspecte un composant de demande limité, mais qui ne gère pas les contenus surdimensionnés comme vous le souhaitez. Pour plus d'informations sur la façon dont les règles AWS gérées gèrent les composants surdimensionnés, consultezAWS Liste des groupes de règles gérées. Pour plus d'informations sur les autres groupes de règles, adressez-vous à votre fournisseur de groupes de règles.

Directives relatives à la gestion des composants surdimensionnés dans votre ACL Web

La façon dont vous gérez les composants surdimensionnés dans votre ACL Web peut dépendre d'un certain nombre de facteurs tels que la taille attendue du contenu des composants de votre demande, le traitement des demandes par défaut de votre ACL Web et la manière dont les autres règles de votre ACL Web correspondent et traitent les demandes.

Les directives générales relatives à la gestion des composants de requêtes Web surdimensionnés sont les suivantes :

- Si vous devez autoriser certaines demandes dont le contenu des composants est surdimensionné, ajoutez si possible des règles pour n'autoriser explicitement que ces demandes. Priorisez ces règles afin qu'elles s'exécutent avant toutes les autres règles de l'ACL Web qui inspectent les mêmes types de composants. Avec cette approche, vous ne pourrez pas AWS WAF inspecter l'intégralité du contenu des composants surdimensionnés que vous autorisez à transmettre à votre ressource protégée.
- Pour toutes les autres demandes, vous pouvez empêcher tout octet supplémentaire de passer en bloquant les demandes qui dépassent la limite :
  - Vos règles et groupes de règles : dans vos règles qui inspectent les composants soumis à des limites de taille, configurez la gestion des surdimensionnements afin de bloquer les demandes dépassant cette limite. Par exemple, si votre règle bloque les demandes dont le contenu d'en-tête est spécifique, définissez la gestion des en-têtes surdimensionnés de manière à ce qu'elle corresponde aux demandes dont le contenu d'en-tête est surdimensionné. Sinon, si votre ACL Web bloque les demandes par défaut et que votre règle autorise un contenu d'en-tête spécifique,

configurez la gestion du surdimensionnement de votre règle pour qu'elle ne corresponde à aucune demande dont le contenu d'en-tête est surdimensionné.

- Groupes de règles que vous ne gérez pas : pour empêcher les groupes de règles que vous ne gérez pas d'autoriser des composants de demande surdimensionnés, vous pouvez ajouter une règle distincte qui inspecte le type de composant de demande et bloque les demandes qui dépassent les limites. Priorisez la règle dans votre ACL Web afin qu'elle s'exécute avant les groupes de règles. Par exemple, vous pouvez bloquer les demandes dont le contenu du corps est surdimensionné avant que l'une de vos règles d'inspection corporelle ne soit exécutée dans l'ACL Web. La procédure suivante décrit comment ajouter ce type de règle.

Blocage des composants de requête Web surdimensionnés

Vous pouvez ajouter une règle dans votre ACL Web qui bloque les demandes contenant des composants surdimensionnés.

Pour ajouter une règle bloquant les contenus surdimensionnés

1. Lorsque vous créez ou modifiez votre ACL Web, dans les paramètres des règles, choisissez Ajouter des règles, Ajouter mes propres règles et groupes de règles, Générateur de règles, puis Éditeur visuel de règles. Pour obtenir des conseils sur la création ou la modification d'une ACL Web, consultezUtilisation des listes ACL web.
2. Entrez un nom pour votre règle et laissez le paramètre Type sur Règle normale.
3. Modifiez les paramètres de correspondance suivants par rapport à leurs valeurs par défaut :

   a. Dans Statement, pour Inspect, ouvrez le menu déroulant et choisissez le composant de requête Web dont vous avez besoin, soit Body, Headers, soit Cookies.

   b. Pour Type de correspondance, choisissez Taille supérieure à.

   c. Pour Taille, tapez un nombre correspondant au moins à la taille minimale pour le type de composant. Pour les en-têtes et les cookies, tapez8192. Dans Application Load Balancer ou dans les ACL AWS AppSync Web, pour les corps, tapez. 8192 Pour les corps dans CloudFront les ACL Web API Gateway, Amazon Cognito, App Runner ou Verified Access, si vous utilisez la limite de taille par défaut, tapez. 16384 Sinon, saisissez la limite de taille que vous avez définie pour votre ACL Web.

   d. Pour la gestion des objets surdimensionnés, sélectionnez Faire correspondre.
4. Pour Action, sélectionnez Bloquer.
5. Choisissez Ajouter une règle.

6. Après avoir ajouté la règle, sur la page Définir la priorité des règles, déplacez-la au-dessus des règles ou des groupes de règles de votre ACL Web qui inspectent le même type de composant. Cela donne à la nouvelle règle un paramètre de priorité numérique inférieur, ce qui oblige AWS WAF à l'évaluer en premier. Pour plus d'informations, voir Ordre de traitement des règles et des groupes de règles dans une ACL Web.

Modèle d'expression régulière correspondant dans AWS WAF

AWS WAF prend en charge la syntaxe des modèles utilisée par la bibliothèque `libpcre` PCRE. La bibliothèque est documentée sur PCRE - Perl Compatible Regular Expressions.

AWS WAF ne prend pas en charge toutes les constructions de la bibliothèque. Par exemple, il prend en charge certaines assertions de largeur nulle, mais pas toutes. Nous ne disposons pas de liste complète des constructions prises en charge. Toutefois, si vous fournissez un modèle d'expression régulière qui n'est pas valide ou si vous utilisez des constructions non prises en charge, l' AWS WAF API signale un échec.

AWS WAF ne prend pas en charge les modèles PCRE suivants :

- Références arrières et capture de sous-expressions
- Références de sous-routines et modèles récursifs
- Modèles conditionnels
- Verbes de contrôle de suivi arrière
- Directive octet unique \C
- Directive de correspondance de nouvelle ligne \R
- Début \K de directive de réinitialisation de correspondance
- Légendes et code intégré
- Regroupement atomique et quantificateurs possessifs

Ensembles d'adresses IP et ensembles de modèles regex dans AWS WAF

AWS WAF stocke des informations plus complexes dans des ensembles que vous utilisez en les référençant dans vos règles. Chacun de ces ensembles a un nom et un ARN (Amazon Resource

Name) lui est attribué lors de sa création. Vous pouvez gérer ces jeux à partir de vos instructions de règles et vous pouvez y accéder et les gérer vous-même, via le volet de navigation de la console.

Vous pouvez utiliser un ensemble géré dans un groupe de règles ou une ACL Web.

- Pour utiliser un ensemble d'adresses IP, voirInstruction de correspondance d'ensemble d'adresses IP de règle.
- Pour utiliser un ensemble de modèles regex, voirInstruction de correspondance d'ensemble de modèles d'expression régulière de règle.

Incohérences temporaires lors des mises à jour

Lorsque vous créez ou modifiez une ACL Web ou d'autres AWS WAF ressources, les modifications mettent peu de temps à se propager à toutes les zones où les ressources sont stockées. Le temps de propagation peut aller de quelques secondes à plusieurs minutes.

Voici des exemples d'incohérences temporaires que vous pourriez remarquer lors de la propagation des modifications :

- Après avoir créé une ACL Web, si vous essayez de l'associer à une ressource, vous pouvez obtenir une exception indiquant que l'ACL Web n'est pas disponible.
- Une fois que vous avez ajouté un groupe de règles à une ACL Web, les nouvelles règles de groupe de règles peuvent être en vigueur dans une zone où l'ACL Web est utilisée et pas dans une autre.
- Une fois que vous avez modifié le paramètre d'une action de règle, vous pouvez voir l'ancienne action à certains endroits et la nouvelle action à d'autres.
- Après avoir ajouté une adresse IP à un ensemble d'adresses IP utilisé dans une règle de blocage, la nouvelle adresse peut être bloquée dans une zone alors qu'elle est toujours autorisée dans une autre.

Rubriques

- Création et gestion d'un ensemble d'adresses IP
- Création et gestion d'un ensemble de modèles d'expression régulière

Création et gestion d'un ensemble d'adresses IP

Un jeu d'adresses IP fournit une collection d'adresses IP et de plages d'adresses IP que vous souhaitez utiliser ensemble dans une instruction de règle. Les ensembles d'adresses IP sont AWS des ressources.

Pour utiliser un ensemble d'adresses IP dans une ACL Web ou un groupe de règles, vous devez d'abord créer une AWS ressource `IPSet` avec les spécifications de votre adresse. Ensuite, vous référencez l'ensemble lorsque vous ajoutez une instruction de règle d'ensemble d'adresses IP à une liste ACL web ou un groupe de règles.

Rubriques

Création d'un ensemble d'adresses IP

Suivez la procédure décrite dans cette section pour créer un nouvel ensemble d'adresses IP.

> **Note**
>
> En plus de la procédure décrite dans cette section, vous avez la possibilité d'ajouter un nouvel ensemble d'adresses IP lorsque vous ajoutez une règle de correspondance IP à votre liste ACL web ou groupe de règles. Pour choisir cette option, vous devez fournir les mêmes paramètres que ceux requis par cette procédure.

Pour créer un ensemble d'adresses IP

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, choisissez Jeux d'adresses IP puis Créer un jeu d'adresses IP.
3. Saisissez un nom et une description pour le jeu d'adresses. Vous les utiliserez pour identifier l'ensemble lorsque vous souhaitez l'utiliser.

> **Note**
>
> Vous ne pouvez pas modifier le nom une fois que vous créez l'ensemble d'adresses IP.

4. Pour Région, choisissez Global (CloudFront) ou choisissez la région dans laquelle vous souhaitez stocker l'ensemble d'adresses IP. Vous pouvez utiliser des ensembles d'adresses IP régionaux uniquement dans les ACL Web qui protègent les ressources régionales. Pour utiliser une adresse IP définie dans les ACL Web qui protègent les CloudFront distributions Amazon, vous devez utiliser Global (CloudFront).
5. Pour Version IP, sélectionnez la version à utiliser.
6. Dans la zone de texte Adresses IP, entrez une adresse IP ou une plage d'adresses IP par ligne, en notation CIDR. AWS WAF prend en charge toutes les plages d'adresses CIDR IPv4 et IPv6, à l'exception de. `/0` Pour plus d'informations sur la notation CIDR, consultez l'article Classless Inter-Domain Routing sur Wikipédia (en anglais).

   Voici quelques exemples :

   - Pour spécifier l'adresse IPv4 192.0.2.44, tapez 192.0.2.44/32.
   - Pour spécifier l'adresse IPv6 2620:0:2 d 0:200:0:0:0:0, tapez 2620:0:2 d 0:200:0:0:0:0 /128.
   - Pour spécifier la plage d'adresses IPv4 de 192.0.2.0 à 192.0.2.255, tapez 192.0.2.0/24.
   - Pour spécifier la plage d'adresses IPv6 de 2620:0:2d0:200:0:0:0:0 à 2620:0:2d0:200:ffff:ffff:ffff:ffff, saisissez 2620:0:2d0:200::/64.
7. Vérifiez les paramètres du jeu d'adresses IP, puis choisissez Créer un jeu d'adresses IP.

Suppression d'un ensemble d'adresses IP

Suivez les instructions de cette section pour supprimer un ensemble référencé.

Suppression d'ensembles et de groupes de règles référencés

Lorsque vous supprimez une entité que vous pouvez utiliser dans une ACL Web, telle qu'un ensemble d'adresses IP, un ensemble de modèles regex ou un groupe de règles, AWS WAF vérifie si l'entité est actuellement utilisée dans une ACL Web. S'il constate qu'il est en cours d'utilisation, il vous AWS WAF avertit. AWS WAF est presque toujours capable de déterminer si une entité est référencée par une ACL Web. Cependant, dans de rares cas, il peut ne pas être en mesure de le faire. Si vous devez être sûr que rien n'utilise actuellement l'entité, vérifiez-la dans vos ACL Web

avant de la supprimer. Si l'entité est un ensemble référencé, vérifiez également qu'aucun groupe de règles ne l'utilise.

Pour supprimer un ensemble d'adresses IP

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le panneau de navigation, choisissez Ensembles d'adresses IP.
3. Sélectionnez le jeu d'adresses IP à supprimer et choisissez Supprimer.

Création et gestion d'un ensemble de modèles d'expression régulière

Un ensemble de modèles regex fournit une collection d'expressions régulières que vous souhaitez utiliser ensemble dans une instruction de règle. Les ensembles de modèles Regex sont des AWS ressources.

Pour utiliser un modèle d'expression régulière défini dans une ACL Web ou un groupe de règles, vous devez d'abord créer une AWS ressource, `RegexPatternSet` avec les spécifications de votre modèle d'expression régulière. Ensuite, vous référencez l'ensemble lorsque vous ajoutez une instruction de règle d'ensemble de modèles regex à une liste ACL web ou un groupe de règles. Un ensemble de modèles regex doit contenir au moins un modèle regex.

Si votre ensemble de modèles d'expressions régulières contient plusieurs modèles d'expressions régulières, lorsqu'il est utilisé dans une règle, la correspondance des modèles est associée `OR` à la logique. Autrement dit, une demande web correspondra à l'instruction de règle de l'ensemble de modèles si le composant de demande correspond à l'un des modèles de l'ensemble.

AWS WAF prend en charge la syntaxe des modèles utilisée par la bibliothèque PCRE, `libpcre` à quelques exceptions près. La bibliothèque est documentée sur PCRE - Perl Compatible Regular Expressions. Pour plus d'informations sur AWS WAF le support, consultezModèle d'expression régulière correspondant dans AWS WAF.

Rubriques

- Création d'un ensemble de modèles d'expression régulière
- Suppression d'un ensemble de modèles d'expression régulière

Création d'un ensemble de modèles d'expression régulière

Suivez la procédure décrite dans cette section pour créer un nouveau ensemble de modèles regex.

Pour créer un ensemble de modèles regex

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le panneau de navigation, choisissez Ensembles de modèles regex, puis Créer un ensemble de modèles regex.
3. Entrez un nom et une description pour l'ensemble de modèles regex. Vous les utiliserez pour l'identifier lorsque vous souhaitez utiliser l'ensemble.

   > **Note**
   >
   > Vous ne pouvez pas modifier le nom après avoir créé l'ensemble de modèles regex.

4. Pour Région, choisissez Global (CloudFront) ou choisissez la région dans laquelle vous souhaitez stocker le jeu de modèles regex. Vous pouvez utiliser des ensembles de modèles regex régionaux uniquement dans les ACL Web qui protègent les ressources régionales. Pour utiliser un modèle regex défini dans les ACL Web qui protègent les CloudFront distributions Amazon, vous devez utiliser Global ()CloudFront.
5. Dans la zone de texte Expressions régulières, entrez un modèle regex par ligne.

   Par exemple, l'expression régulière `I[a@]mAB[a@]dRequest` correspond aux chaînes suivantes : `IamABadRequest`, `IamAB@dRequest`, `I@mABadRequest` et `I@mAB@dRequest`.

   AWS WAF prend en charge la syntaxe des modèles utilisée par la bibliothèque PCRE, `libpcre` à quelques exceptions près. La bibliothèque est documentée sur PCRE - Perl Compatible Regular Expressions. Pour plus d'informations sur AWS WAF le support, consultezModèle d'expression régulière correspondant dans AWS WAF.
6. Passez en revue les paramètres de l'ensemble de modèles regex et choisissez Créer un ensemble de modèles regex.

Suppression d'un ensemble de modèles d'expression régulière

Suivez les instructions de cette section pour supprimer un ensemble référencé.

Suppression d'ensembles et de groupes de règles référencés

Lorsque vous supprimez une entité que vous pouvez utiliser dans une ACL Web, telle qu'un ensemble d'adresses IP, un ensemble de modèles regex ou un groupe de règles, AWS WAF vérifie si l'entité est actuellement utilisée dans une ACL Web. S'il constate qu'il est en cours d'utilisation, il vous AWS WAF avertit. AWS WAF est presque toujours capable de déterminer si une entité est référencée par une ACL Web. Cependant, dans de rares cas, il peut ne pas être en mesure de le faire. Si vous devez être sûr que rien n'utilise actuellement l'entité, vérifiez-la dans vos ACL Web avant de la supprimer. Si l'entité est un ensemble référencé, vérifiez également qu'aucun groupe de règles ne l'utilise.

Pour supprimer un ensemble de modèles regex

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le panneau de navigation, choisissez Ensembles de modèles regex.
3. Sélectionnez l'ensemble de modèles regex que vous souhaitez supprimer et choisissez Supprimer.

Demandes et réponses Web personnalisées dans AWS WAF

Vous pouvez ajouter un comportement personnalisé de gestion des demandes et des réponses Web à vos actions de AWS WAF règles et à vos actions ACL Web par défaut. Vos paramètres personnalisés s'appliquent chaque fois que l'action à laquelle ils sont associés s'applique.

Vous pouvez personnaliser les demandes et réponses Web de la manière suivante :

- AvecAllow, CountCAPTCHA, et Challenge actions, vous pouvez insérer des en-têtes personnalisés dans la requête Web. Lorsque AWS WAF la demande Web est transmise à la ressource protégée, celle-ci contient l'intégralité de la demande d'origine ainsi que les en-têtes personnalisés que vous avez insérés. Pour les Challenge actions CAPTCHA et, applique la personnalisation AWS WAF uniquement si la demande passe le CAPTCHA ou l'inspection du jeton de défi.

- Avec Block les actions, vous pouvez définir une réponse personnalisée complète, avec le code de réponse, les en-têtes et le corps. La ressource protégée répond à la demande en utilisant la réponse personnalisée fournie par AWS WAF. Votre réponse personnalisée remplace la réponse Block d'action par défaut de`403 (Forbidden)`.

Paramètres d'action que vous pouvez personnaliser

Vous pouvez spécifier une demande ou une réponse personnalisée lorsque vous définissez les paramètres d'action suivants :

- Action de la règle. Pour plus d'informations, consultez Action de la règle.
- Action par défaut pour une ACL Web. Pour plus d'informations, consultez L'action par défaut de l'ACL Web.

Paramètres d'action que vous ne pouvez pas personnaliser

Vous ne pouvez pas spécifier un traitement personnalisé des demandes dans l'action de remplacement pour un groupe de règles que vous utilisez dans une ACL Web. veuillez consulter Évaluation des règles ACL Web et des groupes de règles. Voir également Instruction de groupe de règles géré etInstruction de groupe de règles.

Incohérences temporaires lors des mises à jour

Lorsque vous créez ou modifiez une ACL Web ou d'autres AWS WAF ressources, les modifications mettent peu de temps à se propager à toutes les zones où les ressources sont stockées. Le temps de propagation peut aller de quelques secondes à plusieurs minutes.

Voici des exemples d'incohérences temporaires que vous pourriez remarquer lors de la propagation des modifications :

- Après avoir créé une ACL Web, si vous essayez de l'associer à une ressource, vous pouvez obtenir une exception indiquant que l'ACL Web n'est pas disponible.
- Une fois que vous avez ajouté un groupe de règles à une ACL Web, les nouvelles règles de groupe de règles peuvent être en vigueur dans une zone où l'ACL Web est utilisée et pas dans une autre.
- Une fois que vous avez modifié le paramètre d'une action de règle, vous pouvez voir l'ancienne action à certains endroits et la nouvelle action à d'autres.
- Après avoir ajouté une adresse IP à un ensemble d'adresses IP utilisé dans une règle de blocage, la nouvelle adresse peut être bloquée dans une zone alors qu'elle est toujours autorisée dans une autre.

Limites relatives à votre utilisation de demandes et de réponses personnalisées

AWS WAF définit les paramètres maximaux pour votre utilisation des demandes et réponses personnalisées. Par exemple, un nombre maximum d'en-têtes de demande par ACL Web ou groupe de règles, et un nombre maximum d'en-têtes personnalisés pour une seule définition de réponse personnalisée. Pour plus d'informations, consultez AWS WAF quotas.

Rubriques

- Insertions d'en-têtes de demande personnalisées pour les actions non bloquantes
- Réponses personnalisées pour les Block actions
- Codes d'état pris en charge pour une réponse personnalisée

Insertions d'en-têtes de demande personnalisées pour les actions non bloquantes

Vous pouvez demander d' AWS WAF insérer des en-têtes personnalisés dans la requête HTTP d'origine lorsqu'une action de règle ne bloque pas la demande. Avec cette option, vous ne faites qu'ajouter des éléments à la demande. Vous ne pouvez ni modifier ni remplacer aucune partie de la demande initiale. Les cas d'utilisation de l'insertion d'en-têtes personnalisés incluent le fait de signaler à une application en aval de traiter la demande différemment en fonction des en-têtes insérés et de marquer la demande pour analyse.

Cette option s'applique aux actions de règles AllowCount,CAPTCHA, Challenge et aux actions par défaut de l'ACL Web définies surAllow. Pour plus d'informations sur les actions de règle, consultez Action de la règle. Pour plus d'informations sur les actions ACL Web par défaut, consultezL'action par défaut de l'ACL Web.

Noms d'en-têtes de demande personnalisés

AWS WAF préfixe tous les en-têtes de demande qu'il insère`x-amzn-waf-`, afin d'éviter toute confusion avec les en-têtes déjà présents dans la demande. Par exemple, si vous spécifiez le nom de l'en-tête`sample`, AWS WAF insère l'en-tête`x-amzn-waf-sample`.

En-têtes portant le même nom

Si la demande contient déjà un en-tête du même nom qui AWS WAF est en cours d'insertion, AWS WAF remplace l'en-tête. Ainsi, si vous définissez des en-têtes dans plusieurs règles portant des noms identiques, l'en-tête de la dernière règle permettant d'inspecter la demande et de trouver une correspondance sera ajouté, contrairement aux règles précédentes.

En-têtes personnalisés avec actions de règles non terminales

Contrairement à l'Allowaction, l'Countaction ne s'arrête pas au traitement AWS WAF de la requête Web en utilisant les autres règles de l'ACL Web. De même, lorsque vous CAPTCHA Challenge déterminez que le jeton de demande est valide, ces actions n'arrêtent pas le traitement AWS WAF de la demande Web. Ainsi, si vous insérez des en-têtes personnalisés à l'aide d'une règle comportant l'une de ces actions, les règles suivantes peuvent également insérer des en-têtes personnalisés. Pour plus d'informations sur le comportement des actions relatives aux règles, consultezAction de la règle.

Supposons, par exemple, que vous disposiez des règles suivantes, classées par ordre de priorité dans l'ordre indiqué :

1. RuleA avec une Count action et un en-tête personnalisé nommés`RuleAHeader`.
2. RuleB avec une Allow action et un en-tête personnalisé nommés. `RuleBHeader`

Si une demande correspond à la fois à la règle A et à la règle B, AWS WAF insère les en-têtes`x-amzn-waf-RuleBHeader`, `x-amzn-waf-RuleAHeader` puis transmet la demande à la ressource protégée.

AWS WAF insère des en-têtes personnalisés dans une requête Web lorsqu'il a fini d'inspecter la demande. Ainsi, si vous utilisez le traitement personnalisé des demandes avec une règle dont l'action est définie surCount, les en-têtes personnalisés que vous ajoutez ne sont pas inspectés par les règles suivantes.

Exemple de gestion personnalisée des demandes

Vous définissez le traitement personnalisé des demandes pour l'action d'une règle ou pour l'action par défaut d'une ACL Web. La liste suivante montre le JSON pour la gestion personnalisée ajouté à l'action par défaut pour une ACL Web.

```
{
 "Name": "SampleWebACL",
 "Scope": "REGIONAL",
 "DefaultAction": {
  "Allow": {
   "CustomRequestHandling": {
    "InsertHeaders": [
     {
```

```
      "Name": "fruit",
      "Value": "watermelon"
     },
     {
      "Name": "pie",
      "Value": "apple"
     }
    ]
   }
  }
 },
 "Description": "Sample web ACL with custom request handling configured for default
 action.",
 "Rules": [],
 "VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "SampleWebACL"
 }
}
```

Réponses personnalisées pour les Block actions

Vous pouvez demander de AWS WAF renvoyer une réponse HTTP personnalisée au client pour les actions de règle ou les actions par défaut de l'ACL Web définies sur. Block Pour plus d'informations sur les actions de règle, consultez Action de la règle. Pour plus d'informations sur les actions ACL Web par défaut, consultezL'action par défaut de l'ACL Web.

Lorsque vous définissez une gestion personnalisée des réponses pour une Block action, vous définissez le code d'état, les en-têtes et le corps de la réponse. Pour obtenir la liste des codes d'état que vous pouvez utiliser AWS WAF, consultez la section suivante,Codes d'état pris en charge pour une réponse personnalisée.

Cas d’utilisation

Les cas d'utilisation des réponses personnalisées sont les suivants :

- Renvoyer un code d'état autre que celui par défaut au client.
- Renvoi d'en-têtes de réponse personnalisés au client. Vous pouvez spécifier n'importe quel nom d'en-tête, à l'exception de`content-type`.
- Renvoi d'une page d'erreur statique au client.

- Redirection du client vers une autre URL. Pour ce faire, vous spécifiez l'un des codes d'état de `3xx` redirection, tel que `301 (Moved Permanently)` ou`302 (Found)`, puis vous spécifiez un nouvel en-tête `Location` portant le nom de la nouvelle URL.

Interaction avec les réponses que vous définissez dans votre ressource protégée

Les réponses personnalisées que vous spécifiez pour l' AWS WAF Blockaction ont priorité sur les spécifications de réponse que vous définissez dans votre ressource protégée.

Le service hôte de la AWS ressource que vous protégez AWS WAF peut permettre un traitement personnalisé des réponses aux requêtes Web. Voici quelques exemples :

- Avec Amazon CloudFront, vous pouvez personnaliser la page d'erreur en fonction du code d'état. Pour plus d'informations, consultez la section Génération de réponses d'erreur personnalisées dans le manuel Amazon CloudFront Developer Guide.
- Avec Amazon API Gateway, vous pouvez définir le code de réponse et de statut de votre passerelle. Pour plus d'informations, consultez les réponses de Gateway dans API Gateway dans le manuel Amazon API Gateway Developer Guide.

Vous ne pouvez pas combiner AWS WAF des paramètres de réponse personnalisés avec des paramètres de réponse personnalisés dans la AWS ressource protégée. La spécification de réponse pour toute demande Web individuelle provient entièrement AWS WAF ou entièrement de la ressource protégée.

Pour les requêtes Web AWS WAF bloquées, voici l'ordre de priorité.

1. AWS WAF réponse personnalisée — Si une réponse personnalisée est activée pour l' AWS WAF Blockaction, la ressource protégée renvoie la réponse personnalisée configurée au client. Les paramètres de réponse que vous avez éventuellement définis dans la ressource protégée elle-même n'ont aucun effet.
2. Réponse personnalisée définie dans la ressource protégée : sinon, si des paramètres de réponse personnalisés sont spécifiés pour la ressource protégée, la ressource protégée utilise ces paramètres pour répondre au client.
3. AWS WAF Blockréponse par défaut — Dans le cas contraire, la ressource protégée répond au client avec la Block réponse AWS WAF par défaut`403 (Forbidden)`.

Pour les requêtes Web qui le AWS WAF permettent, votre configuration de la ressource protégée détermine la réponse qu'elle renvoie au client. Vous ne pouvez pas configurer les paramètres de réponse AWS WAF pour les demandes autorisées. La seule personnalisation que vous pouvez configurer AWS WAF pour les demandes autorisées est l'insertion d'en-têtes personnalisés dans la demande d'origine, avant de la transmettre à la ressource protégée. Cette option est décrite dans la section précédente,Insertions d'en-têtes de demande personnalisées pour les actions non bloquantes.

En-têtes de réponse personnalisés

Vous pouvez spécifier n'importe quel nom d'en-tête, à l'exception de`content-type`.

Organismes de réponse personnalisés

Vous définissez le corps d'une réponse personnalisée dans le contexte de l'ACL Web ou du groupe de règles dans lequel vous souhaitez l'utiliser. Après avoir défini un corps de réponse personnalisé, vous pouvez l'utiliser par référence à n'importe quel autre endroit de l'ACL Web ou du groupe de règles dans lequel vous l'avez créé. Dans les paramètres Block d'action individuels, vous faites référence au corps personnalisé que vous souhaitez utiliser et vous définissez le code d'état et l'en-tête de la réponse personnalisée.

Lorsque vous créez une réponse personnalisée dans la console, vous pouvez choisir parmi les corps de réponse que vous avez déjà définis ou créer un nouveau corps. En dehors de la console, vous définissez vos corps de réponse personnalisés au niveau de l'ACL Web ou du groupe de règles, puis vous les référencez à partir des paramètres d'action de l'ACL Web ou du groupe de règles. Cela est illustré dans l'exemple JSON de la section suivante.

Exemple de réponse personnalisée

L'exemple suivant répertorie le JSON d'un groupe de règles avec des paramètres de réponse personnalisés. Le corps de réponse personnalisé est défini pour l'ensemble du groupe de règles, puis référencé par une touche dans l'action de règle.

```
{
 "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
}
```

```
}
```

Codes d'état pris en charge pour une réponse personnalisée

Pour des informations détaillées sur les codes d'état HTTP, voir Codes d'état de l'Internet Engineering Task Force (IETF) et Liste des codes de statut HTTP sur Wikipedia.

Les codes d'état HTTP suivants prennent en AWS WAF charge les réponses personnalisées.

- 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 étiquettes sur les requêtes Web

Une étiquette est une métadonnée ajoutée à une demande Web par une règle lorsque la règle correspond à la demande. Une fois ajoutée, une étiquette reste disponible sur la demande jusqu'à la fin de l'évaluation de l'ACL Web. Vous pouvez accéder aux libellés dans les règles qui seront exécutées ultérieurement dans le cadre de l'évaluation de l'ACL Web à l'aide d'une instruction label match. Pour plus de détails, consultez Déclaration relative à la règle de correspondance des étiquettes.

Les étiquettes figurant sur les requêtes Web génèrent des statistiques relatives aux CloudWatch étiquettes Amazon. Pour obtenir la liste des mesures et des dimensions, voirMétriques et dimensions des étiquettes. Pour plus d'informations sur l'accès aux métriques et aux résumés des métriques via CloudWatch et via la AWS WAF console, consultezSurveillance et réglage.

Cas d'utilisation de l'étiquetage

Les cas d'utilisation courants des AWS WAF étiquettes sont les suivants :

- Évaluation d'une demande Web par rapport à plusieurs instructions de règle avant d'agir sur la demande — Une fois qu'une correspondance est trouvée avec une règle dans une ACL Web, AWS WAF continue d'évaluer la demande par rapport à l'ACL Web si l'action de règle ne met pas

fin à l'évaluation de l'ACL Web. Vous pouvez utiliser des étiquettes pour évaluer et collecter des informations issues de plusieurs règles avant de décider d'autoriser ou de bloquer la demande. Pour ce faire, modifiez les actions de vos règles existantes Count et configurez-les pour ajouter des étiquettes aux demandes correspondantes. Ajoutez ensuite une ou plusieurs nouvelles règles à exécuter après vos autres règles, puis configurez-les pour évaluer les étiquettes et gérer les demandes en fonction des combinaisons de correspondance des étiquettes.

- Gestion des requêtes Web par région géographique — Vous pouvez utiliser uniquement la règle de correspondance géographique pour gérer les demandes Web par pays d'origine. Pour affiner l'emplacement au niveau de la région, vous utilisez la règle de correspondance géographique avec une Count action suivie d'une règle de correspondance des étiquettes. Pour plus d'informations sur la règle de correspondance géographique, consultezInstruction de correspondance géographique de règle.
- Réutilisation de la logique entre plusieurs règles : si vous devez réutiliser la même logique pour plusieurs règles, vous pouvez utiliser des étiquettes pour obtenir une source unique de la logique et simplement tester les résultats. Lorsque plusieurs règles complexes utilisent un sous-ensemble commun d'instructions de règles imbriquées, la duplication de l'ensemble de règles communes entre vos règles complexes peut prendre du temps et être source d'erreurs. Avec les étiquettes, vous pouvez créer une nouvelle règle avec le sous-ensemble de règles communes qui compte les demandes correspondantes et leur ajoute une étiquette. Vous ajoutez la nouvelle règle à votre ACL Web afin qu'elle s'exécute avant vos règles complexes d'origine. Ensuite, dans vos règles d'origine, vous remplacez le sous-ensemble de règles partagées par une règle unique qui vérifie l'étiquette.

  Supposons, par exemple, que vous souhaitiez appliquer plusieurs règles uniquement à vos chemins de connexion. Plutôt que de demander à chaque règle de spécifier la même logique pour correspondre aux chemins de connexion potentiels, vous pouvez implémenter une nouvelle règle unique contenant cette logique. Demandez à la nouvelle règle d'ajouter une étiquette aux demandes correspondantes pour indiquer que la demande se trouve sur un chemin de connexion. Dans votre ACL Web, attribuez à cette nouvelle règle un paramètre de priorité numérique inférieur à celui de vos règles d'origine afin qu'elle s'exécute en premier. Ensuite, dans vos règles d'origine, remplacez la logique partagée par une vérification de la présence de l'étiquette. Pour plus d'informations sur les paramètres de priorité, voirOrdre de traitement des règles et des groupes de règles dans une ACL Web.
- Création d'exceptions aux règles dans les groupes de règles : cette option est particulièrement utile pour les groupes de règles gérés, que vous ne pouvez ni afficher ni modifier. De nombreuses règles de groupes de règles gérés ajoutent des étiquettes aux requêtes Web correspondantes, pour indiquer les règles correspondantes et éventuellement pour fournir des informations

supplémentaires sur la correspondance. Lorsque vous utilisez un groupe de règles qui ajoute des étiquettes aux demandes, vous pouvez remplacer les règles du groupe de règles pour compter les correspondances, puis exécuter une règle après le groupe de règles qui gère la demande Web en fonction des étiquettes du groupe de règles. Toutes les règles AWS gérées ajoutent des étiquettes aux requêtes Web correspondantes. Pour plus de détails, consultez les descriptions des règles à l'adresseAWS Liste des groupes de règles gérées.

- Utilisation des métriques d'étiquette pour surveiller les modèles de trafic : vous pouvez accéder aux métriques relatives aux étiquettes que vous ajoutez par le biais de vos règles et aux métriques ajoutées par les groupes de règles gérés que vous utilisez dans votre ACL Web. Tous les groupes de règles AWS gérées ajoutent des étiquettes aux requêtes Web qu'ils évaluent. Pour obtenir la liste des mesures et des dimensions des étiquettes, consultezMétriques et dimensions des étiquettes. Vous pouvez accéder aux métriques et aux résumés des métriques par CloudWatch le biais de la page Web ACL de la AWS WAF console. Pour plus d'informations, veuillez consulter Surveillance et réglage.

Comment fonctionne AWS WAF l'étiquetage

Lorsqu'une règle correspond à une demande Web, si des étiquettes sont définies pour la règle, AWS WAF ajoute les étiquettes à la demande à la fin de l'évaluation de la règle. Les règles évaluées après la règle correspondante dans l'ACL Web peuvent correspondre aux étiquettes ajoutées par la règle.

Qui ajoute des libellés aux demandes

Les composants Web ACL qui évaluent les demandes peuvent ajouter des étiquettes aux demandes.

- Toute règle qui n'est pas une déclaration de référence de groupe de règles peut ajouter des étiquettes aux requêtes Web correspondantes. Les critères d'étiquetage font partie de la définition de la règle, et lorsqu'une requête Web correspond à la règle, AWS WAF ajoute les étiquettes de la règle à la demande. Pour plus d'informations, veuillez consulter the section called “Règles qui ajoutent des étiquettes”.
- L'instruction de règle de correspondance géographique ajoute des libellés de pays et de région à toutes les demandes qu'elle inspecte, que la déclaration aboutisse ou non à une correspondance. Pour plus d'informations, veuillez consulter the section called “Correspondance géographique”.
- Les règles AWS gérées pour AWS WAF tous ajoutent des étiquettes aux demandes qu'ils inspectent. Ils ajoutent des étiquettes en fonction des correspondances de règles dans le groupe de règles et d'autres en fonction des AWS processus utilisés par les groupes de règles gérés, tels que l'étiquetage jeton ajouté lorsque vous utilisez un groupe de règles d'atténuation intelligente des

menaces. Pour plus d'informations sur les étiquettes ajoutées par chaque groupe de règles géré, consultezthe section called “AWS Liste des groupes de règles gérées”.

Comment AWS WAF gère les étiquettes

AWS WAF ajoute les libellés de la règle à la demande à la fin de l'inspection de la demande par la règle. L'étiquetage fait partie des activités de correspondance d'une règle, tout comme l'action.

Les étiquettes ne sont pas conservées dans la requête Web une fois l'évaluation de l'ACL Web terminée. Pour que les autres règles correspondent à une étiquette ajoutée par votre règle, votre action de règle ne doit pas mettre fin à l'évaluation de la requête Web par l'ACL Web. L'action de la règle doit être définie sur CountCAPTCHA, ouChallenge. Lorsque l'évaluation de l'ACL Web ne se termine pas, les règles suivantes de l'ACL Web peuvent exécuter leurs critères de correspondance d'étiquette par rapport à la demande. Pour plus d'informations sur les actions de règle, consultez Action de la règle.

Accès aux étiquettes lors de l'évaluation de l'ACL Web

Une fois ajoutées, les étiquettes restent disponibles sur la demande tant que celle-ci AWS WAF est évaluée par rapport à l'ACL Web. Toute règle d'une ACL Web peut accéder aux étiquettes qui ont été ajoutées par les règles déjà exécutées dans la même ACL Web. Cela inclut les règles définies directement dans l'ACL Web et les règles définies dans les groupes de règles utilisés dans l'ACL Web.

- Vous pouvez effectuer une comparaison avec une étiquette figurant dans les critères d'inspection des demandes de votre règle à l'aide de l'instruction de correspondance des étiquettes. Vous pouvez faire correspondre n'importe quelle étiquette attachée à la demande. Pour plus de détails sur le relevé, voirDéclaration relative à la règle de correspondance des étiquettes.
- L'instruction de correspondance géographique ajoute des étiquettes avec ou sans correspondance, mais elles ne sont disponibles qu'une fois que la règle ACL Web contenant l'instruction a terminé l'évaluation de la demande.
  - Vous ne pouvez pas utiliser une seule règle, par exemple une `AND` instruction logique, pour exécuter une instruction de correspondance géographique suivie d'une instruction de correspondance d'étiquettes par rapport aux étiquettes géographiques. Vous devez placer l'instruction label match dans une règle distincte qui s'exécute après la règle contenant l'instruction Geo Match.
  - Si vous utilisez une instruction de correspondance géographique comme instruction de délimitation dans une déclaration de règle basée sur le taux ou une déclaration de référence

à un groupe de règles géré, les étiquettes ajoutées par l'instruction de correspondance géographique ne peuvent pas être inspectées par l'instruction de la règle qui les contient. Si vous devez inspecter l'étiquetage géographique dans une déclaration de règle basée sur les taux ou dans un groupe de règles, vous devez exécuter l'instruction de correspondance géographique dans une règle distincte qui s'exécute au préalable.

Accès aux informations relatives aux étiquettes en dehors de l'évaluation des ACL sur le Web

Les étiquettes ne sont pas conservées dans la requête Web une fois l'évaluation de l'ACL Web terminée, mais AWS WAF enregistrent les informations relatives aux étiquettes dans les journaux et dans les métriques.

- AWS WAF stocke les CloudWatch statistiques Amazon pour les 100 premières étiquettes sur chaque demande. Pour plus d'informations sur l'accès aux métriques relatives aux étiquettes, reportez-vous aux Surveillance avec Amazon CloudWatch sections etMétriques et dimensions des étiquettes.
- AWS WAF résume les métriques CloudWatch d'étiquette dans les tableaux de bord d'aperçu du trafic ACL Web de la AWS WAF console. Vous pouvez accéder aux tableaux de bord sur n'importe quelle page Web ACL. Pour plus d’informations, consultez Tableaux de bord de présentation du trafic Web ACL.
- AWS WAF enregistre les étiquettes dans les journaux pour les 100 premières étiquettes sur demande. Vous pouvez utiliser des étiquettes, ainsi que l'action des règles, pour filtrer les journaux qui AWS WAF enregistrent. Pour plus d’informations, veuillez consulter Journalisation AWS WAF du trafic ACL Web.

Votre évaluation ACL Web peut appliquer plus de 100 étiquettes à une requête Web et les comparer à plus de 100 étiquettes, mais AWS WAF n'enregistre que les 100 premières dans les journaux et les métriques.

AWS WAF syntaxe des étiquettes et exigences de dénomination

Une étiquette est une chaîne composée d'un préfixe, d'espaces de noms facultatifs et d'un nom. Les composants d'une étiquette sont délimités par deux points. Les étiquettes présentent les exigences et caractéristiques suivantes :

- Les étiquettes distinguent les majuscules et minuscules.
- Chaque espace de noms d'étiquette ou nom d'étiquette peut comporter jusqu'à 128 caractères.

- Vous pouvez spécifier jusqu'à cinq espaces de noms dans une étiquette.
- Les composants d'une étiquette sont séparés par deux points (`:`).
- Vous ne pouvez pas utiliser les chaînes réservées suivantes dans les espaces de noms ou le nom que vous spécifiez pour une étiquette : `awswaf` `awswaf`,,`rulegroup`,`webacl`, `regexpatternsetipset`, et`managed`.

Syntaxe des étiquettes

Une étiquette entièrement qualifiée possède un préfixe, des espaces de noms facultatifs et un nom d'étiquette. Le préfixe identifie le groupe de règles ou le contexte de la liste ACL web de la règle qui a ajouté l'étiquette. Les espaces de noms peuvent être utilisés pour ajouter du contexte à l'étiquette. Le nom de l'étiquette fournit le niveau de détail le plus bas pour une étiquette. Il indique souvent la règle spécifique qui a ajouté l'étiquette à la demande.

Le préfixe de l'étiquette varie en fonction de son origine.

- Vos étiquettes : ce qui suit montre la syntaxe complète des étiquettes que vous créez dans votre ACL Web et dans les règles de groupe de règles. Les types d'entités sont `rulegroup` et`webacl`.

  ```
  awswaf:<entity owner account id>:<entity type>:<entity name>:<custom
   namespace>:...:<label name>
  ```

  - Préfixe de l'espace de noms de l'étiquette : `awswaf:<entity owner account id>:<entity type>:<entity name>:`
  - Ajouts d'espaces de noms personnalisés : `<custom namespace>:…:`

  Lorsque vous définissez une étiquette pour une règle dans un groupe de règles ou une ACL Web, vous contrôlez les chaînes d'espace de noms personnalisées et le nom de l'étiquette. Le reste est généré pour vous par AWS WAF. AWS WAF préfixe automatiquement toutes les étiquettes avec `awswaf` les paramètres d'entité du compte et de l'ACL Web ou du groupe de règles.
- Étiquettes de groupes de règles gérés : ce qui suit montre la syntaxe complète des étiquettes créées par des règles dans des groupes de règles gérés.

  ```
  awswaf:managed:<vendor>:<rule group name>:<custom namespace>:...:<label name>
  ```

  - Préfixe de l'espace de noms de l'étiquette : `awswaf:managed:<vendor>:<rule group name>:`

- Ajouts d'espaces de noms personnalisés : `<custom namespace>:…:`

Tous les groupes de règles AWS gérées ajoutent des étiquettes. Pour de plus amples informations sur les groupes de règles gérées, reportez-vous à la section Groupes de règles gérés.

- Étiquettes provenant d'autres AWS processus : ces processus sont utilisés par les groupes de règles AWS gérées. Ils sont donc ajoutés aux demandes Web que vous évaluez à l'aide de groupes de règles gérés. Vous trouverez ci-dessous la syntaxe complète des étiquettes créées par des processus appelés par des groupes de règles gérés.

```
awswaf:managed:<process>:<custom namespace>:...:<label name>
```

  - Préfixe de l'espace de noms de l'étiquette : `awswaf:managed:<process>:`
  - Ajouts d'espaces de noms personnalisés : `<custom namespace>:…:`

  Les étiquettes de ce type sont répertoriées pour les groupes de règles gérés qui appellent le AWS processus. Pour de plus amples informations sur les groupes de règles gérées, reportez-vous à la section Groupes de règles gérés.

Exemples d'étiquettes pour vos règles

Les exemples d'étiquettes suivants sont définis par les règles d'un groupe de règles nommé `testRules` qui appartient au compte, 111122223333.

```
awswaf:111122223333:rulegroup:testRules:testNS1:testNS2:LabelNameA
```

```
awswaf:111122223333:rulegroup:testRules:testNS1:LabelNameQ
```

```
awswaf:111122223333:rulegroup:testRules:LabelNameZ
```

La liste suivante présente un exemple de spécification d'étiquette au format JSON. Ces noms d'étiquette incluent des chaînes d'espace de noms personnalisées avant le nom d'étiquette de fin.

```
Rule: {
    Name: "label_rule",
    Statement: {...}
    RuleLabels: [
        Name: "header:encoding:utf8",
```

```
        Name: "header:user_agent:firefox"
    ],
    Action: { Count: {} }
}
```

> **Note**
>
> Vous pouvez accéder à ce type de liste dans la console via l'éditeur JSON de règles.

Si vous exécutez la règle précédente dans le même groupe de règles et le même compte que les exemples d'étiquettes précédents, les étiquettes complètes obtenues seront les suivantes :

```
awswaf:111122223333:rulegroup:testRules:header:encoding:utf8
```

```
awswaf:111122223333:rulegroup:testRules:header:user_agent:firefox
```

Exemples d'étiquettes pour les groupes de règles gérés

Vous trouverez ci-dessous des exemples d'étiquettes provenant des groupes de règles AWS Managed Rules et des processus qu'ils invoquent.

```
awswaf:managed:aws:core-rule-set:NoUserAgent_Header
```

```
awswaf:managed:aws:sql-database:SQLiExtendedPatterns_QueryArguments
```

```
awswaf:managed:aws:atp:aggregate:attribute:compromised_credentials
```

```
awswaf:managed:token:accepted
```

AWS WAF règles qui ajoutent des étiquettes

Dans presque toutes les règles, vous pouvez définir des étiquettes et AWS WAF les appliquer à toute demande correspondante.

Les types de règles suivants constituent les seules exceptions :

- Les règles basées sur le taux n'étiquettent que lorsque le débit est limité : les règles basées sur le taux ajoutent uniquement des étiquettes aux demandes Web pour une instance d'agrégation spécifique lorsque cette instance est limitée par. AWS WAF Pour plus d'informations sur les règles basées sur les taux, consultezInstruction de règle basée sur un taux.
- L'étiquetage n'est pas autorisé dans les instructions de référence des groupes de règles : la console n'accepte pas les libellés pour ces types de règles. Par le biais de l'API, la spécification d'une étiquette pour l'un ou l'autre type d'instruction entraîne une exception de validation. Pour plus d'informations sur ces types d'instructions, reportez-vous Instruction de groupe de règles géré aux sections etInstruction de groupe de règles.

WCU : 1 WCU pour 5 étiquettes que vous définissez dans votre ACL Web ou vos règles de groupe de règles.

Où chercher

- Générateur de règles sur la console : dans les paramètres d'action de la règle, sous Label.
- Type de données d'API — `Rule` `RuleLabels`

Vous définissez une étiquette dans une règle en spécifiant les chaînes d'espace de nommage personnalisées et le nom à ajouter au préfixe d'espace de nommage de l'étiquette. AWS WAF dérive le préfixe du contexte dans lequel vous définissez la règle. Pour plus d'informations à ce sujet, consultez les informations sur la syntaxe des étiquettes sousAWS WAF syntaxe des étiquettes et exigences de dénomination.

AWS WAF règles qui correspondent aux libellés

Vous pouvez utiliser une instruction de correspondance des libellés pour évaluer les libellés des requêtes Web. Vous pouvez effectuer une comparaison avec Label, qui nécessite le nom de l'étiquette, ou avec Namespace, qui nécessite une spécification d'espace de noms. Pour l'étiquette ou l'espace de noms, vous pouvez éventuellement inclure les espaces de noms précédents et le préfixe dans votre spécification. Pour des informations générales sur ce type d'instruction, consultezDéclaration relative à la règle de correspondance des étiquettes.

Le préfixe d'une étiquette définit le contexte du groupe de règles ou de l'ACL Web dans lequel la règle de l'étiquette est définie. Dans l'instruction de correspondance d'étiquette d'une règle, si votre chaîne de correspondance d'étiquette ou d'espace de noms ne spécifie pas le préfixe, AWS WAF utilise le préfixe de la règle de correspondance d'étiquette.

- Les étiquettes des règles définies directement dans une ACL Web ont un préfixe qui spécifie le contexte de l'ACL Web.
- Les libellés des règles faisant partie d'un groupe de règles comportent un préfixe qui indique le contexte du groupe de règles. Il peut s'agir de votre propre groupe de règles ou d'un groupe de règles géré pour vous.

Pour plus d'informations à ce sujet, voir la syntaxe des étiquettes sousAWS WAF syntaxe des étiquettes et exigences de dénomination.

> **Note**
>
> Certains groupes de règles gérés ajoutent des libellés. Vous pouvez les récupérer via l'API en appelant`DescribeManagedRuleGroup`. Les étiquettes sont répertoriées dans la `AvailableLabels` propriété de la réponse.

Si vous souhaitez effectuer une comparaison avec une règle située dans un contexte différent de celui de votre règle, vous devez fournir le préfixe dans votre chaîne de correspondance. Par exemple, si vous souhaitez effectuer une comparaison avec les libellés ajoutés par les règles d'un groupe de règles géré, vous pouvez ajouter une règle dans votre ACL Web avec une instruction de correspondance d'étiquette dont la chaîne de correspondance indique le préfixe du groupe de règles suivi de vos critères de correspondance supplémentaires.

Dans la chaîne de correspondance pour l'instruction label match, vous spécifiez une étiquette ou un espace de noms :

- Étiquette — La spécification de l'étiquette pour une correspondance comprend la partie terminale de l'étiquette. Vous pouvez inclure n'importe quel nombre d'espaces de noms contigus qui précèdent immédiatement le nom de l'étiquette suivi du nom. Vous pouvez également fournir l'étiquette entièrement qualifiée en commençant la spécification par le préfixe.

  Exemples de spécifications :

  - `testNS1:testNS2:LabelNameA`
  - `awswaf:managed:aws:managed-rule-set:testNS1:testNS2:LabelNameA`
- Espace de noms — La spécification d'espace de noms pour une correspondance se compose de tout sous-ensemble contigu de la spécification de l'étiquette, à l'exception du nom. Vous pouvez inclure le préfixe et inclure une ou plusieurs chaînes d'espace de noms.

Exemples de spécifications :

- `testNS1:testNS2:`
- `awswaf:managed:aws:managed-rule-set:testNS1:`

AWS WAF exemples de correspondance d'étiquettes

Cette section fournit des exemples de spécifications de correspondance, pour l'instruction de règle de correspondance des étiquettes.

> **Note**
>
> Ces listes JSON ont été créées dans la console en ajoutant une règle à une ACL Web avec l'étiquette correspondant aux spécifications, puis en modifiant la règle et en passant à l'éditeur Rule JSON. Vous pouvez également obtenir le JSON d'un groupe de règles ou d'une ACL Web via les API ou l'interface de ligne de commande.

Rubriques

- Match contre un label local
- Correspondance avec une étiquette provenant d'un autre contexte
- Correspondance avec une étiquette de groupe de règles géré
- Correspondance avec un espace de noms local
- Correspondance avec un espace de noms de groupe de règles géré

Match contre un label local

La liste JSON suivante montre une instruction de correspondance d'étiquette pour une étiquette qui a été ajoutée localement à la requête Web, dans le même contexte que cette règle.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "header:encoding:utf8"
        }
```

```
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Si vous utilisez cette instruction de correspondance dans le compte 111122223333, dans une règle que vous définissez pour l'ACL Web`testWebACL`, elle correspondra aux libellés suivants.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

```
awswaf:111122223333:webacl:testWebACL:testNS1:testNS2:header:encoding:utf8
```

Elle ne correspondrait pas à l'étiquette suivante, car la chaîne d'étiquette ne correspond pas exactement.

```
awswaf:111122223333:webacl:testWebACL:header:encoding2:utf8
```

Il ne correspondrait pas à l'étiquette suivante, car le contexte n'est pas le même, donc le préfixe ne correspond pas. Cela est vrai même si vous avez ajouté le groupe de règles `productionRules` à l'ACL Web`testWebACL`, où la règle est définie.

```
awswaf:111122223333:rulegroup:productionRules:header:encoding:utf8
```

Correspondance avec une étiquette provenant d'un autre contexte

La liste JSON suivante montre une règle de correspondance d'étiquette qui correspond à une étiquette d'une règle au sein d'un groupe de règles créé par l'utilisateur. Le préfixe est obligatoire dans la spécification pour toutes les règles exécutées dans l'ACL Web qui ne font pas partie du groupe de règles nommé. Cet exemple de spécification d'étiquette correspond uniquement à l'étiquette exacte.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:111122223333:rulegroup:testRules:header:encoding:utf8"
        }
```

```
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Correspondance avec une étiquette de groupe de règles géré

Il s'agit d'un cas particulier de correspondance avec une étiquette provenant d'un autre contexte que celui de la règle de correspondance. La liste JSON suivante montre une instruction de correspondance d'étiquette pour une étiquette de groupe de règles géré. Cela correspond uniquement à l'étiquette exacte spécifiée dans le paramètre clé de l'instruction label match.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "LABEL",
            Key: "awswaf:managed:aws:managed-rule-set:header:encoding:utf8"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Correspondance avec un espace de noms local

La liste JSON suivante montre une instruction label match pour un espace de noms local.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "header:encoding:"
        }
    },
    Labels: [
        ...generate_more_labels...
    ],
```

```
    Action: { Block: {} }
}
```

Comme pour la `Label` correspondance locale, si vous utilisez cette instruction dans le compte 111122223333, dans une règle que vous définissez pour l'ACL Web`testWebACL`, elle correspondra à l'étiquette suivante.

```
awswaf:111122223333:webacl:testWebACL:header:encoding:utf8
```

Il ne correspondrait pas à l'étiquette suivante, car le compte n'est pas le même, donc le préfixe ne correspond pas.

```
awswaf:444455556666:webacl:testWebACL:header:encoding:utf8
```

Le préfixe ne correspond pas non plus aux libellés appliqués par les groupes de règles gérés, comme indiqué ci-dessous.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

Correspondance avec un espace de noms de groupe de règles géré

La liste JSON suivante montre une instruction de correspondance d'étiquette pour un espace de noms de groupe de règles géré. Pour un groupe de règles dont vous êtes le propriétaire, vous devez également fournir le préfixe afin de correspondre à un espace de noms situé en dehors du contexte de la règle.

```
Rule: {
    Name: "match_rule",
    Statement: {
        LabelMatchStatement: {
            Scope: "NAMESPACE",
            Key: "awswaf:managed:aws:managed-rule-set:header:"
        }
    },
    RuleLabels: [
        ...generate_more_labels...
    ],
    Action: { Block: {} }
}
```

Cette spécification correspond aux exemples d'étiquettes suivants.

```
awswaf:managed:aws:managed-rule-set:header:encoding:utf8
```

```
awswaf:managed:aws:managed-rule-set:header:encoding:unicode
```

Il ne correspond pas à l'étiquette suivante.

```
awswaf:managed:aws:managed-rule-set:query:badstring
```

AWS WAF Atténuation intelligente des menaces

Cette section couvre les fonctionnalités intelligentes gérées d'atténuation des menaces fournies par AWS WAF. Il s'agit de protections avancées et spécialisées que vous pouvez mettre en œuvre pour vous protéger contre les menaces telles que les robots malveillants et les tentatives de prise de contrôle de compte.

> **Note**
>
> Les fonctionnalités décrites ici entraînent des coûts supplémentaires, au-delà des frais d'utilisation AWS WAF de base. Pour plus d'informations, consultez Tarification d'AWS WAF.

Les conseils fournis dans cette section sont destinés aux utilisateurs qui savent généralement comment créer et gérer des ACL, des règles et des groupes de règles AWS WAF Web. Ces sujets sont abordés dans les sections précédentes de ce guide.

Rubriques

- Options pour une atténuation intelligente des menaces
- Meilleures pratiques pour une atténuation intelligente des menaces
- AWS WAF jetons de demande Web
- AWS WAF Contrôle des fraudes : création de comptes, prévention des fraudes (ACFP)
- AWS WAF Contrôle des fraudes et prévention des prises de contrôle des comptes (ATP)
- AWS WAF Contrôle des robots
- AWS WAF intégration d'applications clientes
- CAPTCHAet Challenge dans AWS WAF

Options pour une atténuation intelligente des menaces

Cette section fournit une comparaison détaillée des options de mise en œuvre d'une atténuation intelligente des menaces.

AWS WAF propose les types de protection suivants pour une atténuation intelligente des menaces.

- AWS WAF Contrôle des fraudes et prévention des fraudes à la création de comptes (ACFP) : détecte et gère les tentatives de création de compte malveillantes sur la page d'inscription de votre application. Les fonctionnalités de base sont fournies par le groupe de règles géré par l'ACFP. Pour plus d'informations, consultez AWS WAF Contrôle des fraudes : création de comptes, prévention des fraudes (ACFP) et AWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes.
- AWS WAF Prévention du piratage de compte Fraud Control (ATP) : détecte et gère les tentatives de piratage malveillantes sur la page de connexion de votre application. Les fonctionnalités de base sont fournies par le groupe de règles géré par ATP. Pour plus d'informations, consultez AWS WAF Contrôle des fraudes et prévention des prises de contrôle des comptes (ATP) et AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP).
- AWS WAF Contrôle des robots — Identifie, étiquette et gère les robots sympathiques et malveillants. Cette fonctionnalité permet de gérer les robots courants dont les signatures sont uniques dans toutes les applications, ainsi que les robots ciblés dont les signatures sont spécifiques à une application. Les fonctionnalités de base sont fournies par le groupe de règles géré par Bot Control. Pour plus d'informations, consultez AWS WAF Contrôle des robots et AWS WAF Groupe de règles Bot Control.
- SDK d'intégration d'applications clientes : validez les sessions client et les utilisateurs finaux sur vos pages Web et acquérez AWS WAF des jetons que les clients pourront utiliser dans leurs requêtes Web. Si vous utilisez ACFP, ATP ou Bot Control, implémentez les SDK d'intégration d'applications dans votre application cliente si possible, afin de tirer pleinement parti de toutes les fonctionnalités des groupes de règles. Nous recommandons d'utiliser ces groupes de règles sans intégration du SDK uniquement à titre de mesure temporaire, lorsqu'une ressource critique doit être rapidement sécurisée et qu'il n'y a pas assez de temps pour intégrer le SDK. Pour plus d'informations sur la mise en œuvre des SDK, consultezAWS WAF intégration d'applications clientes.
- Challengeet actions CAPTCHA relatives aux règles : validez les sessions des clients et les utilisateurs finaux et obtenez AWS WAF des jetons que les clients pourront utiliser dans leurs requêtes Web. Vous pouvez les implémenter partout où vous spécifiez une action de règle, dans vos règles et en tant que dérogations dans les groupes de règles que vous utilisez. Ces

actions utilisent des AWS WAF JavaScript interstitiels pour interroger le client ou l'utilisateur final, et elles nécessitent des applications clientes qui les prennent en charge. JavaScript Pour plus d'informations, consultez CAPTCHAet Challenge dans AWS WAF.

Les groupes de règles AWS Managed Rules d'atténuation intelligente des menaces ACFP, ATP et Bot Control utilisent des jetons pour une détection avancée. Pour plus d'informations sur les fonctionnalités activées par les jetons dans les groupes de règles, reportez-vous aux Pourquoi utiliser les SDK d'intégration d'applications avec ATP sectionsPourquoi utiliser les SDK d'intégration d'applications avec ACFP, etPourquoi utiliser les SDK d'intégration d'applications avec Bot Control.

Vos options pour mettre en œuvre une atténuation intelligente des menaces vont de l'utilisation de base d'actions de règles pour relever des défis et imposer l'acquisition de jetons, aux fonctionnalités avancées offertes par les groupes de règles de AWS gestion des règles d'atténuation intelligente des menaces.

Les tableaux suivants fournissent des comparaisons détaillées des options pour les fonctionnalités de base et avancées.

Rubriques

- Options pour les défis et l'acquisition de jetons
- Options pour l'atténuation intelligente des menaces, groupes de règles gérés
- Options de limitation du débit dans les règles basées sur les taux et dans les règles de contrôle des bots ciblées

Options pour les défis et l'acquisition de jetons

Vous pouvez proposer des défis et acquérir des jetons à l'aide des SDK d'intégration d' AWS WAF applications ou des actions de règles Challenge etCAPTCHA. D'une manière générale, les actions relatives aux règles sont plus faciles à mettre en œuvre, mais elles entraînent des coûts supplémentaires, s'immiscent davantage sur votre expérience client et sont obligatoires. JavaScript Les SDK nécessitent une programmation dans vos applications clientes, mais ils peuvent offrir une meilleure expérience client, ils sont gratuits et peuvent être utilisés avec JavaScript ou dans des applications Android ou iOS. Vous ne pouvez utiliser les SDK d'intégration d'applications qu'avec des ACL Web qui utilisent l'un des groupes de règles gérés payants d'atténuation intelligente des menaces, décrits dans la section suivante.

Comparaison des options pour les défis et l'acquisition de jetons

	Action de règle Challenge	Action de règle CAPTCHA	JavaScript Défi du SDK	Défi du SDK mobile
Qu'est-ce que c'est	Règle : action qui impose l'acquisition du AWS WAF jeton en présentant au client du navigateur un défi silencieux (interstitiel)	Règle : action qui impose l'acquisition du AWS WAF jeton en présentant à l'utilisateur final un défi visuel ou audio (interstitiel)	Couche d'intégration des applications, pour les navigateurs clients et les autres appareils qui s'exécutentJavaScript. Lance le défi silencieux et obtient un jeton	Couche d'intégration des applications, pour les applications Android et iOS. Rend nativement le défi silencieux et obtient un jeton
Bon choix pour...	Validation silencieuse contre les sessions de bots et application de l'acquisition de jetons pour les clients qui prennent en charge JavaScript	Validation silencieuse par l'utilisateur final contre les sessions de bot et application de l'acquisition de jetons, pour les clients qui prennent en charge JavaScript	Validation silencieuse contre les sessions de bots et mise en œuvre de l'acquisition de jetons pour les clients qui les prennent en charge JavaScript. Les SDK offrent la latence la plus faible et le meilleur contrôle sur l'endroit où le script de défi	Validation silencieuse contre les sessions de bots et application de l'acquisition de jetons pour les applications mobiles natives sur Android et iOS. Les SDK offrent la latence la plus faible et le meilleur contrôle sur l'endroit où le script de défi s'exécute dans l'application.

	Action de règle Challenge	Action de règle CAPTCHA	JavaScript Défi du SDK	Défi du SDK mobile
			s'exécute dans l'application.	
Considérations relatives à la	Implémenté en tant que règle, paramètre d'action	Implémenté en tant que règle, paramètre d'action	Nécessite l'un des groupes de règles payants ACFP, ATP ou Bot Control de l'ACL Web. Nécessite un codage dans l'application client.	Nécessite l'un des groupes de règles payants ACFP, ATP ou Bot Control de l'ACL Web. Nécessite un codage dans l'application client.
Considérations concernant l'exécution	Flux intrusif pour les demandes sans jetons valides. Le client est redirigé vers un interstitiel de AWS WAF challenge. Ajoute des allers-retours sur le réseau et nécessite une deuxième évaluation de la requête Web.	Flux intrusif pour les demandes sans jetons valides. Le client est redirigé vers un AWS WAF interstitiel CAPTCHA. Ajoute des allers-retours sur le réseau et nécessite une deuxième évaluation de la requête Web.	Peut être exécuté dans les coulisses. Vous permet de mieux contrôler l'expérience du défi.	Peut être exécuté dans les coulisses. Vous permet de mieux contrôler l'expérience du défi.
Requiert JavaScript	Oui	Oui	Oui	Non

	Action de règle Challenge	Action de règle CAPTCHA	JavaScript Défi du SDK	Défi du SDK mobile
Clients pris en charge	Navigateur et appareils qui exécutent Javascript	Navigateur et appareils qui exécutent Javascript	Navigateur et appareils qui exécutent Javascript	Appareils Android et iOS
Supporte les applications d'une seule page (SPA)	Exécution uniquement. Vous pouvez utiliser cette Challenge action conjointement avec les SDK pour vous assurer que les demandes contiennent un jeton de défi valide. Vous ne pouvez pas utiliser l'action de règle pour envoyer le script de défi à la page.	Exécution uniquement. Vous pouvez utiliser cette CAPTCHA action conjointement avec les SDK pour vous assurer que les demandes contiennent un jeton CAPTCHA valide. Vous ne pouvez pas utiliser l'action de règle pour envoyer le script CAPTCHA à la page.	Oui	N/A

	Action de règle Challenge	Action de règle CAPTCHA	JavaScript Défi du SDK	Défi du SDK mobile
Coût supplémentaire	Oui, pour les paramètres d'action que vous spécifiez explicitement, soit dans les règles que vous définissez, soit en tant que dérogation aux actions des règles dans les groupes de règles que vous utilisez. Non dans tous les autres cas.	Oui, pour les paramètres d'action que vous spécifiez explicitement, soit dans les règles que vous définissez, soit en tant que dérogation aux actions des règles dans les groupes de règles que vous utilisez. Non dans tous les autres cas.	Non, mais nécessite l'un des groupes de règles payants ACFP, ATP ou Bot Control.	Non, mais nécessite l'un des groupes de règles payants ACFP, ATP ou Bot Control.

Pour plus de détails sur les coûts associés à ces options, consultez les informations relatives à l'atténuation intelligente des menaces sur la page AWS WAF Tarification.

Il peut être plus simple de lancer des défis et d'appliquer les jetons de base en ajoutant simplement une règle avec une CAPTCHA action Challenge ou. Vous devrez peut-être utiliser les actions des règles, par exemple si vous n'avez pas accès au code de l'application.

Cependant, si vous pouvez implémenter les SDK, vous pouvez réduire les coûts et réduire le temps de latence dans votre évaluation ACL Web des requêtes Web des clients, par rapport à l'utilisation de l'Challengeaction suivante :

- Vous pouvez écrire l'implémentation de votre SDK pour exécuter le défi à n'importe quel moment de votre application. Vous pouvez acquérir le jeton en arrière-plan, avant toute action du client susceptible d'envoyer une demande Web à votre ressource protégée. De cette façon, le jeton peut être envoyé avec la première demande de votre client.

- Si, au contraire, vous acquérez des jetons en implémentant une règle avec l'Challengeaction, la règle et l'action nécessitent une évaluation et un traitement supplémentaires des requêtes Web lorsque le client envoie une demande pour la première fois et chaque fois que le jeton expire. L'Challengeaction bloque la demande qui ne contient pas de jeton valide et non expiré et renvoie l'interstitiel de défi au client. Une fois que le client a répondu avec succès au défi, l'interstitiel renvoie la demande Web d'origine avec le jeton valide, qui est ensuite évalué une deuxième fois par l'ACL Web.

Options pour l'atténuation intelligente des menaces, groupes de règles gérés

Les groupes de règles AWS gérées pour l'atténuation intelligente des menaces permettent de gérer les robots de base, de détecter et d'atténuer les robots malveillants sophistiqués, de détecter et d'atténuer les tentatives de prise de contrôle de comptes, ainsi que de détecter et d'atténuer les tentatives de création de comptes frauduleuses. Ces groupes de règles, combinés aux SDK d'intégration d'applications décrits dans la section précédente, fournissent les protections les plus avancées et un couplage sécurisé avec vos applications clientes.

Comparaison des options de groupes de règles gérées

	ACFP	ATP	Bot Control (niveau commun)	Niveau ciblé de Bot Control
Qu'est-ce que c'est	Gère les demandes susceptibles de faire partie de tentatives de création de compte frauduleuses sur les pages d'inscription et d'inscription d'une application.	Gère les demandes susceptibles de faire partie de tentatives de prise de contrôle malveillantes sur la page de connexion d'une application. Ne gère pas les robots.	Gère les robots courants qui s'identifient eux-mêmes, avec des signatures uniques pour toutes les applications. veuillez consulter AWS WAF Groupe de règles Bot Control.	Gère les robots ciblés qui ne s'identifient pas eux-mêmes, avec des signatures spécifiques à une application. veuillez consulter AWS WAF Groupe de règles Bot Control.

	ACFP	ATP	Bot Control (niveau commun)	Niveau ciblé de Bot Control
	Ne gère pas les robots. veuillez consulter AWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes.	veuillez consulter AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP).		

	ACFP	ATP	Bot Control (niveau commun)	Niveau ciblé de Bot Control
Bon choix pour...	L'inspection du trafic de création de comptes pour détecter toute création de compte frauduleuse attaque les tentatives de création de tels comptes en passant par le nom d'utilisateur et en créant de nombreux nouveaux comptes à partir d'une seule adresse IP.	L'inspection du trafic de connexion pour détecter le piratage de compte attaque les tentatives de connexion par traversée de mots de passe et les nombreuses tentatives de connexion effectuées à partir de la même adresse IP. Lorsqu'il est utilisé avec des jetons, il fournit également des protections globales telles que la limitation du débit des adresses IP et des sessions client en cas d'échec élevé de tentatives de connexion.	Protection de base contre les bots et étiquetage du trafic de bots courant et automatisé.	Protection ciblée contre les robots sophistiqués, notamment en limitant le débit au niveau de la session client et en détectant et atténuant les outils d'automatisation des navigateurs tels que Selenium et Puppeteer.

	ACFP	ATP	Bot Control (niveau commun)	Niveau ciblé de Bot Control
Ajoute des étiquettes indiquant les résultats de l'évaluation	Oui	Oui	Oui	Oui
Ajoute des étiquettes de jetons	Oui	Oui	Oui	Oui
Blocage des demandes dont le jeton n'est pas valide	Non inclus. veuillez consulter Blocage des demandes dont le AWS WAF jeton n'est pas valide.	Non inclus. veuillez consulter Blocage des demandes dont le AWS WAF jeton n'est pas valide.	Non inclus. veuillez consulter Blocage des demandes dont le AWS WAF jeton n'est pas valide.	Bloque les sessions client qui envoient 5 demandes sans jeton.
Nécessite le AWS WAF jeton `aws-waf-token`	Obligatoire pour toutes les règles. veuillez consulter Pourquoi utiliser les SDK d'intégration d'applications avec ACFP.	Obligatoire pour de nombreuses règles. veuillez consulter Pourquoi utiliser les SDK d'intégration d'applications avec ATP.	Non	Oui

	ACFP	ATP	Bot Control (niveau commun)	Niveau ciblé de Bot Control
Acquiert le AWS WAF jeton `aws-waf-token`	Oui, conformément à la règle `AllRequests`	Non	Non	Certaines règles utilisent Challenge ou CAPTCHA régissent des actions qui permettent d'acquérir des jetons.

Pour plus de détails sur les coûts associés à ces options, consultez les informations relatives à l'atténuation intelligente des menaces sur la page AWS WAF Tarification.

Options de limitation du débit dans les règles basées sur les taux et dans les règles de contrôle des bots ciblées

Le niveau ciblé du groupe de règles AWS WAF Bot Control et l'énoncé de règle AWS WAF basé sur le taux permettent tous deux de limiter le débit des requêtes Web. Le tableau suivant compare les deux options.

Comparaison des options de détection et d'atténuation basées sur le débit

	AWS WAF règle basée sur le taux	AWS WAF Règles ciblées de Bot Control	
Comment la limitation de débit est appliquée	Agit sur des groupes de demandes qui arrivent à un rythme trop élevé. Vous pouvez appliquer n'importe quelle action à l'exception deAllow.	Applique des modèles d'accès similaires à ceux des humains et applique une limitation dynamique du débit, grâce à l'utilisation de jetons de demande.	

	AWS WAF règle basée sur le taux	AWS WAF Règles ciblées de Bot Control	
Sur la base de l'historique du trafic ?	Non	Oui	
Temps nécessaire pour accumuler des données de référence historiques sur le trafic	N/A	Cinq minutes pour les seuils dynamiques. N/A pour jeton absent.	
Retard d'atténuation	Habituellement 30 à 50 secondes. Cela peut prendre plusieurs minutes.	Généralement moins de 10 secondes. Cela peut prendre plusieurs minutes.	
Objectifs d'atténuation	Configurable. Vous pouvez regrouper les demandes à l'aide d'une instruction scope-down et d'une ou de plusieurs clés d'agrégation, telles que l'adresse IP, la méthode HTTP et la chaîne de requête.	Adresses IP et sessions client	
Niveau de volume de trafic requis pour déclencher des mesures d'atténuation	Moyen : le nombre de demandes peut être inférieur à 100 dans le créneau horaire spécifié	Faible : conçu pour détecter les modèles clients tels que les scrapers lents	
Seuils personnalisables	Oui	Non	

	AWS WAF règle basée sur le taux	AWS WAF Règles ciblées de Bot Control	
Action d'atténuation par défaut	La valeur par défaut de la console estBlock. Aucun paramètre par défaut dans l'API ; le paramètre est obligatoire. Vous pouvez définir cette option pour n'importe quelle action de règle, à l'exception deAllow.	Les paramètres d'action des règles du groupe de règles Challenge concernent l'absence de jeton et CAPTCHA le trafic à volume élevé provenant d'une seule session client. Vous pouvez définir l'une ou l'autre de ces règles pour n'importe quelle action de règle valide.	
Résilience face aux attaques hautement distribuées	Moyen : 10 000 adresses IP maximum pour limiter les adresses IP à elle seule	Moyen : limité à 50 000 au total entre les adresses IP et les jetons	
AWS WAF Tarification	Inclus dans les frais standard pour AWS WAF.	Inclus dans les frais correspondant au niveau ciblé d'atténuation intelligente des menaces par Bot Control.	
Pour plus d'informations	Instruction de règle basée sur un taux	AWS WAF Groupe de règles Bot Control	

Meilleures pratiques pour une atténuation intelligente des menaces

Suivez les meilleures pratiques décrites dans cette section pour mettre en œuvre les fonctionnalités intelligentes d'atténuation des menaces de la manière la plus efficace et la plus rentable possible.

- Implémenter les SDK d'intégration des applications mobiles JavaScript et des applications mobiles : implémentez l'intégration des applications pour activer l'ensemble complet des fonctionnalités ACFP, ATP ou Bot Control de la manière la plus efficace possible. Les groupes de règles gérés utilisent les jetons fournis par les SDK pour séparer le trafic client légitime du trafic indésirable au niveau de la session. Les SDK d'intégration des applications garantissent que ces jetons sont toujours disponibles. Pour plus d'informations, consultez la:
  - Pourquoi utiliser les SDK d'intégration d'applications avec ACFP
  - Pourquoi utiliser les SDK d'intégration d'applications avec ATP
  - Pourquoi utiliser les SDK d'intégration d'applications avec Bot Control

  Utilisez les intégrations pour mettre en œuvre les défis de votre client et pour JavaScript personnaliser la façon dont les puzzles CAPTCHA sont présentés à vos utilisateurs finaux. Pour plus de détails, consultez AWS WAF intégration d'applications clientes.

  Si vous personnalisez des puzzles CAPTCHA à l'aide de l' JavaScript API et que vous utilisez l'action de la CAPTCHA règle n'importe où dans votre ACL Web, suivez les instructions relatives à la gestion de la réponse AWS WAF CAPTCHA dans votre client à l'adresse. Gestion d'une réponse CAPTCHA depuis AWS WAF Ces instructions s'appliquent à toutes les règles qui utilisent l'CAPTCHAaction, y compris celles du groupe de règles géré par l'ACFP et le niveau de protection ciblé du groupe de règles géré par Bot Control.
- Limitez les demandes que vous envoyez aux groupes de règles ACFP, ATP et Bot Control : l'utilisation des groupes de règles de règles de AWS gestion des règles d'atténuation intelligente des menaces entraîne des frais supplémentaires. Le groupe de règles ACFP inspecte les demandes adressées aux points de terminaison d'enregistrement et de création de comptes que vous spécifiez. Le groupe de règles ATP inspecte les demandes adressées au point de terminaison de connexion que vous spécifiez. Le groupe de règles Bot Control inspecte chaque demande qui lui parvient lors de l'évaluation de l'ACL Web.

  Envisagez les approches suivantes pour réduire votre utilisation de ces groupes de règles :

  - Exclure les demandes de l'inspection à l'aide d'une instruction scope-down dans l'instruction du groupe de règles géré. Vous pouvez le faire avec n'importe quel énoncé emboîtable. Pour plus d'informations, consultez Déclarations de portée réduite.

- Exclure les demandes de l'inspection en ajoutant des règles avant le groupe de règles. Pour les règles que vous ne pouvez pas utiliser dans une instruction de portée réduite et pour les situations plus complexes, telles que l'étiquetage suivi d'une correspondance d'étiquettes, vous souhaiterez peut-être ajouter des règles qui s'exécutent avant les groupes de règles. Pour plus d'informations, consultez Déclarations de portée réduite et Notions de base sur les énoncés.
- Exécutez les groupes de règles selon des règles moins coûteuses. Si d'autres AWS WAF règles standard bloquent les demandes pour quelque raison que ce soit, exécutez-les avant ces groupes de règles payants. Pour plus d'informations sur les règles et leur gestion, consultezNotions de base sur les énoncés.
- Si vous utilisez plusieurs groupes de règles gérés d'atténuation intelligente des menaces, exécutez-les dans l'ordre suivant pour réduire les coûts : Bot Control, ATP, ACFP.

Pour obtenir des informations détaillées sur la tarification, veuillez consulter la section Tarification AWS WAF.

- Activez le niveau de protection ciblé du groupe de règles Bot Control pendant le trafic Web normal : certaines règles du niveau de protection ciblé ont besoin de temps pour établir des bases de référence pour les modèles de trafic normaux avant de pouvoir reconnaître les modèles de trafic irréguliers ou malveillants et y répondre. Par exemple, les `TGT_ML_*` règles ont besoin de 24 heures pour s'échauffer.

  Ajoutez ces protections lorsque vous n'êtes pas victime d'une attaque et donnez-leur le temps d'établir leurs bases de référence avant de s'attendre à ce qu'ils répondent de manière appropriée aux attaques. Si vous ajoutez ces règles au cours d'une attaque, une fois celle-ci terminée, le temps nécessaire pour établir une base de référence est généralement du double au triple du temps normalement requis, en raison de la distorsion ajoutée par le trafic d'attaque. Pour plus d'informations sur les règles et les temps de préchauffage requis, consultezListe des règles.
- Pour la protection par déni de service distribué (DDoS), utilisez l'atténuation automatique des attaques DDoS au niveau de la couche application Shield Advanced. Les groupes de règles d'atténuation intelligente des menaces ne fournissent pas de protection DDoS. L'ACFP protège contre les tentatives frauduleuses de création de compte sur la page d'inscription de votre application. ATP vous protège contre les tentatives d'usurpation de compte sur votre page de connexion. Bot Control se concentre sur l'application de modèles d'accès de type humain à l'aide de jetons et sur la limitation dynamique du débit lors des sessions client.

  Lorsque vous utilisez Shield Advanced alors que l'atténuation automatique des attaques DDoS au niveau de l'application est activée, Shield Advanced répond automatiquement aux attaques

DDoS détectées en créant, en évaluant et en déployant des mesures d' AWS WAF atténuation personnalisées en votre nom. Pour plus d'informations sur Shield AdvancedAWS Shield Advanced vue d'ensemble, reportez-vous aux sections etAWS Shield Advanced protections de la couche d'application (couche 7).

- Régler et configurer la gestion des jetons : ajustez la gestion des jetons de l'ACL Web pour une expérience utilisateur optimale.
  - Pour réduire les coûts d'exploitation et améliorer l'expérience de votre utilisateur final, réglez les durées d'immunité de gestion des jetons au maximum de vos exigences de sécurité. Cela permet de réduire au minimum l'utilisation de puzzles CAPTCHA et de défis silencieux. Pour plus d'informations, consultez Expiration de l'horodatage : durée d'immunité des AWS WAF jetons.
  - Pour activer le partage de jetons entre des applications protégées, configurez une liste de domaines de jetons pour votre ACL Web. Pour plus d'informations, consultez AWS WAF domaines à jetons et listes de domaines.
- Rejeter les demandes avec des spécifications d'hôte arbitraires : configurez vos ressources protégées pour exiger que `Host` les en-têtes des requêtes Web correspondent à la ressource ciblée. Vous pouvez accepter une valeur ou un ensemble de valeurs spécifique, par exemple `myExampleHost.com` et`www.myExampleHost.com`, mais n'acceptez pas de valeurs arbitraires pour l'hôte.
- Pour les équilibreurs de charge d'application qui sont à l'origine de CloudFront distributions, configurez CloudFront et AWS WAF gérez correctement les jetons : si vous associez votre ACL Web à un Application Load Balancer et que vous déployez l'Application Load Balancer comme origine CloudFront d'une distribution, consultez. Configuration requise pour les équilibreurs de charge d'application qui sont des origines CloudFront
- Testez et ajustez avant le déploiement : avant de mettre en œuvre des modifications dans votre ACL Web, suivez les procédures de test et de réglage décrites dans ce guide pour vous assurer que vous obtenez le comportement que vous attendez. Cela est particulièrement important pour ces fonctionnalités payantes. Pour des conseils généraux, voirTester et ajuster vos AWS WAF protections. Pour obtenir des informations spécifiques aux groupes de règles gérés payants, reportez-vous aux Tester et déployer ATP sectionsTest et déploiement de l'ACFP, etTester et déployer AWS WAF Bot Control.

AWS WAF jetons de demande Web

AWS WAF les jetons font partie intégrante des protections améliorées offertes par l'atténuation AWS WAF intelligente des menaces. Un jeton, parfois appelé empreinte digitale, est un ensemble

d'informations relatives à une session client unique que le client stocke et fournit avec chaque requête Web qu'il envoie. AWS WAF utilise des jetons pour identifier et séparer les sessions client malveillantes des sessions légitimes, même lorsque les deux proviennent d'une seule adresse IP. L'utilisation de jetons impose des coûts négligeables pour les utilisateurs légitimes, mais élevés à grande échelle pour les botnets.

AWS WAF utilise des jetons pour prendre en charge la fonctionnalité de défi de son navigateur et de l'utilisateur final, qui est fournie par les SDK d'intégration des applications et par les actions de règles Challenge etCAPTCHA. En outre, les jetons activent les fonctionnalités des groupes de règles gérés pour le contrôle des AWS WAF bots et la prévention du piratage de comptes.

AWS WAF crée, met à jour et chiffre des jetons pour les clients qui répondent avec succès aux défis silencieux et aux puzzles CAPTCHA. Lorsqu'un client doté d'un jeton envoie une requête Web, celui-ci inclut le jeton crypté, le AWS WAF déchiffre et vérifie son contenu.

Rubriques

Comment AWS WAF utilise les jetons

AWS WAF utilise des jetons pour enregistrer et vérifier les types de validation de session client suivants :

- CAPTCHA — Les puzzles CAPTCHA aident à distinguer les robots des utilisateurs humains. Un CAPTCHA est exécuté uniquement par l'action de la CAPTCHA règle. Une fois le puzzle terminé, le script CAPTCHA met à jour l'horodatage CAPTCHA du jeton. Pour plus d’informations, consultez CAPTCHAet Challenge dans AWS WAF.
- Défi — Les défis s'exécutent en silence pour aider à distinguer les sessions clients ordinaires des sessions de bot et pour rendre le fonctionnement des robots plus coûteux. Lorsque le défi est

terminé avec succès, le script du défi se procure automatiquement un nouveau jeton AWS WAF si nécessaire, puis met à jour l'horodatage du défi du jeton.

AWS WAF lance des défis dans les situations suivantes :

- SDK d'intégration d'applications — Les SDK d'intégration d'applications s'exécutent dans les sessions de votre application cliente et permettent de garantir que les tentatives de connexion ne sont autorisées qu'une fois que le client a répondu avec succès à un défi. Pour plus d'informations, consultez AWS WAF intégration d'applications clientes.
- Challengeaction de la règle — Pour plus d'informations, consultezCAPTCHAet Challenge dans AWS WAF.
- CAPTCHA— Lorsqu'un interstitiel CAPTCHA s'exécute, si le client n'a pas encore de jeton, le script lance d'abord automatiquement un défi, afin de vérifier la session du client et d'initialiser le jeton.

Les jetons sont requis par de nombreuses règles des groupes de règles de règles de AWS gestion des menaces intelligentes. Les règles utilisent des jetons pour distinguer les clients au niveau de la session, pour déterminer les caractéristiques du navigateur et pour comprendre le niveau d'interactivité humaine sur la page Web de l'application. Ces groupes de règles font appel à la gestion des AWS WAF jetons, qui applique un étiquetage des jetons que les groupes de règles inspectent ensuite.

- AWS WAF Contrôle des fraudes, création de comptes, prévention de la fraude (ACFP) : les règles de l'ACFP exigent des requêtes Web avec des jetons valides. Pour plus d'informations sur les règles, consultezAWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes.
- AWS WAF Prévention du piratage de compte (ATP) contre la fraude : les règles ATP qui empêchent les sessions client à volume élevé et de longue durée nécessitent des requêtes Web contenant un jeton valide avec un horodatage de défi non expiré. Pour plus d'informations, consultez AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP).
- AWS WAF Contrôle des robots : les règles ciblées de ce groupe de règles limitent le nombre de requêtes Web qu'un client peut envoyer sans jeton valide, et elles utilisent le suivi des sessions par jeton pour la surveillance et la gestion au niveau des sessions. Selon les besoins, les règles appliquent les actions Challenge et CAPTCHA règles pour renforcer l'acquisition de jetons et le comportement valide des clients. Pour plus d'informations, voir AWS WAF Groupe de règles Bot Control.

AWS WAF caractéristiques du jeton

Chaque jeton possède les caractéristiques suivantes :

- Le jeton est stocké dans un cookie nomméaws-waf-token.
- Le jeton est crypté.
- Le jeton imprime à la session client un identifiant granulaire permanent contenant les informations suivantes :
  - Horodatage de la dernière réponse réussie du client à un défi silencieux.
  - Horodatage de la dernière réponse réussie de l'utilisateur final à un CAPTCHA. Ceci n'est présent que si vous utilisez le CAPTCHA dans vos protections.
  - Informations supplémentaires sur le client et le comportement des clients qui peuvent aider à séparer vos clients légitimes du trafic indésirable. Les informations comprennent divers identificateurs de clients et des signaux côté client qui peuvent être utilisés pour détecter des activités automatisées. Les informations recueillies ne sont pas uniques et ne peuvent pas être associées à un être humain individuel.
    - Tous les jetons incluent des données issues de l'interrogation du navigateur client, telles que des indications d'automatisation et des incohérences dans les paramètres du navigateur. Ces informations sont récupérées par les scripts exécutés par l'Challengeaction et par les SDK des applications clientes. Les scripts interrogent activement le navigateur et placent les résultats dans le jeton.
    - En outre, lorsque vous implémentez un SDK d'intégration d'applications clientes, le jeton inclut des informations collectées passivement sur l'interactivité de l'utilisateur final avec la page de l'application. L'interactivité inclut les mouvements de souris, les pressions sur les touches et les interactions avec tout formulaire HTML présent sur la page. Ces informations permettent de AWS WAF détecter le niveau d'interactivité humaine chez le client, afin de défier les utilisateurs qui ne semblent pas être des humains. Pour plus d'informations sur les intégrations côté client, consultezAWS WAF intégration d'applications clientes.

Pour des raisons de sécurité, AWS ne fournit pas de description complète du contenu des AWS WAF jetons ni d'informations détaillées sur le processus de chiffrement des jetons.

Expiration de l'horodatage : durée d'immunité des AWS WAF jetons

AWS WAF utilise les temps de challenge et d'immunité aux CAPTCHA pour contrôler la fréquence à laquelle une session client unique peut être associée à un défi ou à un CAPTCHA. Une fois

qu'un utilisateur final a répondu avec succès à un CAPTCHA, la durée d'immunité au CAPTCHA détermine la durée pendant laquelle l'utilisateur final reste immunisé contre la présentation d'un autre CAPTCHA. De même, la durée d'immunité au défi détermine la durée pendant laquelle une session client reste à l'abri d'une nouvelle contestation après avoir répondu avec succès à un défi.

AWS WAF enregistre une réponse réussie à un défi ou à un CAPTCHA en mettant à jour l'horodatage correspondant à l'intérieur du jeton. Lorsqu'il AWS WAF inspecte le jeton à la recherche d'un challenge ou d'un CAPTCHA, il soustrait l'horodatage de l'heure actuelle. Si le résultat est supérieur à la durée d'immunité configurée, l'horodatage est expiré.

Vous pouvez configurer les durées d'immunité au défi et au CAPTCHA dans l'ACL Web ainsi que dans toute règle utilisant l'action de la Challenge règle CAPTCHA or.

- Le paramètre ACL Web par défaut pour les deux durées d'immunité est de 300 secondes.
- Vous pouvez spécifier la durée d'immunité pour toute règle utilisant l'Challengeaction CAPTCHA ou. Si vous ne spécifiez pas la durée d'immunité pour la règle, elle hérite du paramètre de l'ACL Web.
- Pour une règle au sein d'un groupe de règles qui utilise l'Challengeaction CAPTCHA ou, si vous ne spécifiez pas le délai d'immunité pour la règle, elle héritera du paramètre de chaque ACL Web sur laquelle vous utilisez le groupe de règles.
- Les SDK d'intégration des applications utilisent le temps d'immunité aux défis de l'ACL Web.

La valeur minimale de la durée d'immunité aux défis est de 300 secondes. La valeur minimale de la durée d'immunité au CAPTCHA est de 60 secondes. La valeur maximale pour les deux durées d'immunité est de 259 200 secondes, soit trois jours.

Vous pouvez utiliser l'ACL Web et les paramètres de durée d'immunité au niveau des règles pour ajuster l'CAPTCHAactionChallenge, ou le comportement de gestion des défis du SDK. Par exemple, vous pouvez configurer des règles qui contrôlent l'accès aux données très sensibles avec des durées d'immunité faibles, puis définir des durées d'immunité plus élevées dans votre ACL Web pour que vos autres règles et les SDK héritent.

En particulier dans le cas du CAPTCHA, résoudre un casse-tête peut dégrader l'expérience de votre client sur le site Web. Le réglage de la durée d'immunité du CAPTCHA peut donc vous aider à atténuer l'impact sur l'expérience client tout en fournissant les protections que vous souhaitez.

Pour plus d'informations sur le réglage des durées d'immunité en fonction de votre utilisation des actions Challenge et des CAPTCHA règles, consultezBonnes pratiques d'utilisation des Challenge actions CAPTCHA et.

Où définir les durées d'immunité des AWS WAF jetons

Vous pouvez définir les durées d'immunité dans votre ACL Web et dans vos règles qui utilisent les actions de CAPTCHA règles Challenge et.

Pour des informations générales sur la gestion d'une ACL Web et de ses règles, consultezUtilisation des listes ACL web.

Où définir la durée d'immunité pour une ACL Web

- Console — Lorsque vous modifiez l'ACL Web, dans l'onglet Règles, modifiez et modifiez les paramètres des volets de configuration CAPTCHA Web ACL et Web ACL Challenge. Dans la console, vous pouvez configurer le CAPTCHA ACL Web et contester les temps d'immunité uniquement après avoir créé l'ACL Web.
- En dehors de la console : le type de données ACL Web contient des paramètres de configuration CAPTCHA et challenge, que vous pouvez configurer et fournir à vos opérations de création et de mise à jour sur l'ACL Web.

Où définir la durée d'immunité pour une règle

- Console — Lorsque vous créez ou modifiez une règle et que vous spécifiez l'Challengeaction CAPTCHA ou, vous pouvez modifier le paramètre de durée d'immunité de la règle.
- En dehors de la console : le type de données de règle comporte des paramètres de configuration CAPTCHA et de défi, que vous pouvez configurer lorsque vous définissez la règle.

AWS WAF domaines à jetons et listes de domaines

Lorsqu'il AWS WAF crée un jeton pour un client, il le configure avec un domaine de jetons. Lorsqu'il AWS WAF inspecte un jeton dans une requête Web, il le rejette comme non valide si son domaine ne correspond à aucun des domaines considérés comme valides pour l'ACL Web.

Par défaut, AWS WAF n'accepte que les jetons dont le paramètre de domaine correspond exactement au domaine hôte de la ressource associée à l'ACL Web. Il s'agit de la valeur de l'`Host`en-tête de la requête Web. Dans un navigateur, vous pouvez trouver ce domaine dans la

JavaScript `window.location.hostname` propriété et dans l'adresse que votre utilisateur voit dans sa barre d'adresse.

Vous pouvez également spécifier des domaines de jetons acceptables dans la configuration de votre ACL Web, comme décrit dans la section suivante. Dans ce cas, AWS WAF accepte à la fois les correspondances exactes avec l'en-tête de l'hôte et les correspondances avec les domaines de la liste des domaines de jetons.

Vous pouvez spécifier les domaines de jetons AWS WAF à utiliser lors de la définition du domaine et lors de l'évaluation d'un jeton dans une ACL Web. Les domaines que vous spécifiez ne peuvent pas être des suffixes publics tels que. `gov.au` Pour les domaines que vous ne pouvez pas utiliser, consultez la liste https://publicsuffix.org/list/public_suffix_list.dat sous Liste des suffixes publics.

AWS WAF configuration de la liste de domaines du jeton ACL Web

Vous pouvez configurer une ACL Web pour partager des jetons entre plusieurs ressources protégées en fournissant une liste de domaines de jetons avec les domaines supplémentaires que vous AWS WAF souhaitez accepter. Avec une liste de domaines de jetons, accepte AWS WAF toujours le domaine hôte de la ressource. En outre, il accepte tous les domaines de la liste des domaines symboliques, y compris leurs sous-domaines préfixés.

Par exemple, une spécification `example.com` de domaine de votre liste de domaines de jetons correspond à `example.com` (from`http://example.com/`)`api.example.com`, (from`http://api.example.com/`) et `www.example.com` (from`http://www.example.com/`). Il ne correspond pas à`example.api.com`, (de`http://example.api.com/`) ou `apiexample.com` (de`http://apiexample.com/`).

Vous pouvez configurer la liste des domaines de jetons dans votre ACL Web lorsque vous la créez ou que vous la modifiez. Pour des informations générales sur la gestion d'une ACL Web, consultezUtilisation des listes ACL web.

AWS WAF paramètres de domaine de jetons

AWS WAF crée des jetons à la demande des scripts de défi, qui sont exécutés par les SDK d'intégration des applications Challenge et les actions de CAPTCHA règles.

Le domaine qui AWS WAF définit un jeton est déterminé par le type de script de défi qui le demande et par toute configuration de domaine de jeton supplémentaire que vous fournissez. AWS WAF définit le domaine du jeton selon le paramètre le plus court et le plus général qu'il puisse trouver dans la configuration.

- JavaScript SDK — Vous pouvez configurer le JavaScript SDK avec une spécification de domaine jeton, qui peut inclure un ou plusieurs domaines. Les domaines que vous configurez doivent être des domaines qui AWS WAF seront acceptés, sur la base du domaine hôte protégé et de la liste des domaines de jetons de l'ACL Web.

  Lorsqu'il AWS WAF émet un jeton pour le client, il définit le domaine du jeton sur celui qui correspond au domaine hôte et qui est le plus court, parmi le domaine hôte et les domaines de votre liste configurée. Par exemple, si le domaine hôte est, `api.example.com` et la liste des domaines de jetons`example.com`, AWS WAF utilise `example.com` le jeton, car il correspond au domaine hôte et est plus court. Si vous ne fournissez pas de liste de domaines de jetons dans la configuration de l' JavaScript AWS WAF API, définissez le domaine sur le domaine hôte de la ressource protégée.

  Pour plus d'informations, consultez Fournir des domaines à utiliser dans les jetons.

- SDK mobile — Dans le code de votre application, vous devez configurer le SDK mobile avec une propriété de domaine jeton. Cette propriété doit être un domaine qui AWS WAF acceptera, sur la base du domaine hôte protégé et de la liste des domaines de jetons de l'ACL Web.

  Lorsqu'il AWS WAF émet un jeton pour le client, celui-ci utilise cette propriété comme domaine du jeton. AWS WAF n'utilise pas le domaine hôte dans les jetons qu'il émet pour le client du SDK mobile.

  Pour plus d'informations, consultez le `WAFConfiguration` `domainName` paramètre surSpécification du SDK AWS WAF mobile.

- Challengeaction — Si vous spécifiez une liste de domaines de jetons dans l'ACL AWS WAF Web, définissez le domaine de jetons sur celui qui correspond au domaine hôte et qui est le plus court, parmi le domaine hôte et les domaines de la liste. Par exemple, si le domaine hôte est, `api.example.com` et la liste des domaines de jetons`example.com`, AWS WAF utilise `example.com` le jeton, car il correspond au domaine hôte et est plus court. Si vous ne fournissez pas de liste de domaines de jetons dans l'ACL Web AWS WAF , définissez le domaine sur le domaine hôte de la ressource protégée.

AWS WAF étiquetage des jetons par le bot et groupes de règles gérés contre la fraude

Cette section décrit les étiquettes que la gestion des AWS WAF jetons ajoute aux requêtes Web. Pour des informations générales sur les étiquettes, voirAWS WAF étiquettes sur les requêtes Web.

Lorsque vous utilisez l'un des AWS WAF robots ou des groupes de règles gérés par le contrôle de la fraude, les groupes de règles utilisent la gestion des AWS WAF jetons pour inspecter les jetons de requête Web et appliquer un étiquetage de jeton aux demandes. Pour plus d'informations sur les groupes de règles gérés, reportez-vous aux AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP) sectionsAWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes, etAWS WAF Groupe de règles Bot Control.

> **Note**
>
> AWS WAF applique des étiquettes de jetons uniquement lorsque vous utilisez l'un de ces groupes de règles gérés d'atténuation intelligente des menaces.

La gestion des jetons peut ajouter les libellés suivants aux requêtes Web.

Libellé de session client

L'étiquette `awswaf:managed:token:id:`*`identifier`* contient un identifiant unique que la gestion des AWS WAF jetons utilise pour identifier la session client. L'identifiant peut changer si le client acquiert un nouveau jeton, par exemple après avoir supprimé le jeton qu'il utilisait.

> **Note**
>
> AWS WAF ne communique pas CloudWatch les statistiques Amazon pour cette étiquette.

Étiquettes d'état des jetons : préfixes d'espace de noms d'étiquettes

Les étiquettes d'état du jeton indiquent le statut du jeton et les informations de défi et de CAPTCHA qu'il contient.

Chaque étiquette de statut de jeton commence par l'un des préfixes d'espace de noms suivants :

- `awswaf:managed:token:` — Utilisé pour signaler l'état général du jeton et pour rendre compte de l'état des informations de défi du jeton.
- `awswaf:managed:captcha:` — Utilisé pour rendre compte de l'état des informations CAPTCHA du jeton.

Étiquettes d'état des jetons : noms des étiquettes

Après le préfixe, le reste de l'étiquette fournit des informations détaillées sur l'état du jeton :

- `accepted`— Le jeton de demande est présent et contient les éléments suivants :
  - Un défi ou une solution CAPTCHA valide.
  - Un défi ou un horodatage CAPTCHA non expiré.
  - Spécification de domaine valide pour l'ACL Web.

  Exemple : L'étiquette `awswaf:managed:token:accepted` indique que le jeton des requêtes Web contient une solution de défi valide, un horodatage de défi non expiré et un domaine valide.
- `rejected`— Le jeton de demande est présent mais ne répond pas aux critères d'acceptation.

  Outre l'étiquette rejetée, la gestion des jetons ajoute un espace de noms et un nom d'étiquette personnalisés pour en indiquer la raison.
  - `rejected:not_solved`— Le challenge ou la solution CAPTCHA ne sont pas présents dans le jeton.
  - `rejected:expired`— L'horodatage du challenge ou du CAPTCHA du jeton a expiré, conformément aux durées d'immunité des jetons configurées par votre ACL Web.
  - `rejected:domain_mismatch`— Le domaine du jeton ne correspond pas à la configuration du domaine du jeton de votre ACL Web.
  - `rejected:invalid`— AWS WAF n'a pas pu lire le jeton indiqué.

  Exemple : les `awswaf:managed:captcha:rejected` libellés `awswaf:managed:captcha:rejected:expired` indiquent que la demande a été rejetée parce que l'horodatage CAPTCHA contenu dans le jeton a dépassé le délai d'immunité du jeton CAPTCHA configuré dans l'ACL Web.
- `absent`— La demande ne contient pas le jeton ou le gestionnaire de jetons n'a pas pu le lire.

  Exemple : L'étiquette `awswaf:managed:captcha:absent` indique que la demande ne contient pas le jeton.

Blocage des demandes dont le AWS WAF jeton n'est pas valide

Lorsque vous utilisez la menace intelligente AWS Managed Rules`AWSManagedRulesACFPRuleSet`, les groupes de règles et `AWSManagedRulesATPRuleSetAWSManagedRulesBotControlRuleSet`, les groupes de règles

invoquent la gestion des AWS WAF jetons pour évaluer le statut du jeton de requête Web et étiqueter les demandes en conséquence.

> **Note**
>
> L'étiquetage des jetons s'applique uniquement aux demandes Web que vous évaluez à l'aide de l'un de ces groupes de règles gérés.

Pour plus d'informations sur l'étiquetage appliqué par la gestion des jetons, consultez la section précédente,AWS WAF étiquetage des jetons par le bot et groupes de règles gérés contre la fraude.

Les groupes de règles gérés d'atténuation intelligente des menaces gèrent ensuite les exigences en matière de jetons comme suit :

- La `AWSManagedRulesACFPRuleSet` `AllRequests` règle est configurée pour exécuter l'Challengeaction sur toutes les demandes, bloquant ainsi efficacement celles qui ne possèdent pas l'étiquette du `accepted` jeton.
- Le `AWSManagedRulesATPRuleSet` bloque les demandes portant le libellé du `rejected` jeton, mais il ne bloque pas les demandes portant le libellé du `absent` jeton.
- Le niveau de protection `AWSManagedRulesBotControlRuleSet` ciblé pose un défi aux clients après avoir envoyé cinq demandes sans étiquette de `accepted` jeton. Il ne bloque pas une demande individuelle dont le jeton n'est pas valide. Le niveau de protection commun du groupe de règles ne gère pas les exigences en matière de jetons.

Pour plus de détails sur les groupes de règles de menaces intelligentesAWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes, reportez-vous aux sections AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP) etAWS WAF Groupe de règles Bot Control.

Pour bloquer les demandes auxquelles il manque des jetons lors de l'utilisation du groupe de règles géré par Bot Control ou ATP

Avec les groupes de règles Bot Control et ATP, il est possible qu'une demande sans jeton valide quitte l'évaluation du groupe de règles et continue d'être évaluée par l'ACL Web.

Pour bloquer toutes les demandes dont le jeton est manquant ou dont le jeton est rejeté, ajoutez une règle à exécuter immédiatement après le groupe de règles géré afin de capturer et de bloquer les demandes que le groupe de règles ne gère pas pour vous.

Voici un exemple de liste JSON pour une ACL Web qui utilise le groupe de règles géré par ATP. L'ACL Web a une règle ajoutée pour capturer l'`awswaf:managed:token:absent`étiquette et la gérer. La règle limite son évaluation aux demandes Web destinées au point de terminaison de connexion, afin de correspondre à l'étendue du groupe de règles ATP. La règle ajoutée est indiquée en gras.

```
{
  "Name": "exampleWebACL",
  "Id": "55555555-6666-7777-8888-999999999999",
  "ARN": "arn:aws:wafv2:us-east-1:111111111111:regional/webacl/
exampleWebACL/55555555-4444-3333-2222-111111111111",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesATPRuleSet",
      "Priority": 1,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesATPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesATPRuleSet": {
                "LoginPath": "/web/login",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  }
                },
                "ResponseInspection": {
                  "StatusCode": {
                    "SuccessCodes": [
```

```
                    200
                  ],
                  "FailureCodes": [
                    401,
                    403,
                    500
                  ]
                }
              }
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesATPRuleSet"
    }
  },
  {
    "Name": "RequireTokenForLogins",
    "Priority": 2,
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "Statement": {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:token:absent"
              }
            }
          },
          {
            "ByteMatchStatement": {
              "SearchString": "/web/login",
              "FieldToMatch": {
                "UriPath": {}
              },
              "TextTransformations": [
```

```
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ],
              "PositionalConstraint": "STARTS_WITH"
            }
          },
          {
            "ByteMatchStatement": {
              "SearchString": "POST",
              "FieldToMatch": {
                "Method": {}
              },
              "TextTransformations": [
                {
                  "Priority": 0,
                  "Type": "NONE"
                }
              ],
              "PositionalConstraint": "EXACTLY"
            }
          }
        ]
      }
    },
    "Action": {
      "Block": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "RequireTokenForLogins"
    }
  }
],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "exampleWebACL"
},
"Capacity": 51,
"ManagedByFirewallManager": false,
"LabelNamespace": "awswaf:111111111111:webacl:exampleWebACL:"
```

```
}
```

Configuration requise pour les équilibreurs de charge d'application qui sont des origines CloudFront

Lisez cette section si vous associez votre ACL Web à un Application Load Balancer et que vous déployez l'Application Load Balancer comme origine d'une distribution. CloudFront

Avec cette architecture, vous devez fournir la configuration supplémentaire suivante pour que les informations du jeton soient traitées correctement.

- Configurez CloudFront pour transférer le `aws-waf-token` cookie vers l'Application Load Balancer. CloudFront Supprime par défaut les cookies de la requête Web avant de la transmettre à l'origine. Pour conserver le cookie jeton dans la requête Web, configurez le comportement du CloudFront cache pour inclure uniquement le cookie jeton ou tous les cookies. Pour plus d'informations sur la procédure à suivre, consultez la section Mise en cache du contenu basé sur les cookies dans le manuel Amazon CloudFront Developer Guide.
- Configurez de AWS WAF manière à ce qu'il reconnaisse le domaine de la CloudFront distribution comme un domaine de jeton valide. Par défaut, CloudFront définit l'`Host`en-tête sur l'origine de l'Application Load Balancer et l' AWS WAF utilise comme domaine de la ressource protégée. Le navigateur client considère toutefois la CloudFront distribution comme le domaine hôte, et les jetons générés pour le client utilisent le CloudFront domaine comme domaine de jeton. Sans configuration supplémentaire, lorsque le domaine AWS WAF de ressources protégé est comparé au domaine de jeton, il y aura une incompatibilité. Pour résoudre ce problème, ajoutez le nom CloudFront de domaine de distribution à la liste des domaines de jetons dans votre configuration ACL Web. Pour plus d'informations sur la procédure à utiliser, consultez AWS WAF configuration de la liste de domaines du jeton ACL Web.

AWS WAF Contrôle des fraudes : création de comptes, prévention des fraudes (ACFP)

La fraude liée à la création de compte est une activité illégale en ligne dans le cadre de laquelle un attaquant tente de créer un ou plusieurs faux comptes. Les attaquants utilisent de faux comptes pour des activités frauduleuses, telles que l'utilisation abusive de bonus promotionnels et d'inscription, l'usurpation d'identité de quelqu'un et des cyberattaques telles que le phishing. La présence de faux comptes peut avoir un impact négatif sur votre entreprise en portant atteinte à votre réputation auprès des clients et en vous exposant à des fraudes financières.

Vous pouvez surveiller et contrôler les tentatives de fraude liées à la création de comptes en mettant en œuvre la fonction de prévention des AWS WAF fraudes liées à la création de comptes Fraud Control (ACFP). AWS WAF propose cette fonctionnalité dans le groupe de règles AWS Managed Rules `AWSManagedRulesACFPRuleSet` avec des SDK d'intégration d'applications complémentaires.

L'ACFP a géré les groupes de règles pour étiqueter et gérer les demandes susceptibles de faire partie de tentatives de création de compte malveillantes. Pour ce faire, le groupe de règles inspecte les tentatives de création de compte que les clients envoient au point de terminaison de création de compte de votre application.

L'ACFP protège les pages d'ouverture de votre compte en surveillant les demandes d'ouverture de compte pour détecter toute activité anormale et en bloquant automatiquement les demandes suspectes. Le groupe de règles utilise des identifiants de demande, une analyse comportementale et l'apprentissage automatique pour détecter les demandes frauduleuses.

- Inspection des demandes — L'ACFP vous donne de la visibilité et un contrôle sur les tentatives de création de compte anormales et les tentatives utilisant des informations d'identification volées, afin d'empêcher la création de comptes frauduleux. L'ACFP vérifie les combinaisons d'e-mails et de mots de passe par rapport à sa base de données d'identifiants volés, qui est régulièrement mise à jour à mesure que de nouvelles informations d'identification divulguées sont découvertes sur le Dark Web. L'ACFP évalue les domaines utilisés dans les adresses e-mail et surveille l'utilisation des numéros de téléphone et des champs d'adresse afin de vérifier les entrées et de détecter les comportements frauduleux. L'ACFP agrège les données par adresse IP et par session client afin de détecter et de bloquer les clients qui envoient trop de demandes suspectes.
- Inspection des réponses — Pour les CloudFront distributions, en plus d'inspecter les demandes de création de compte entrantes, le groupe de règles ACFP inspecte les réponses de votre application aux tentatives de création de compte, afin de suivre les taux de réussite et d'échec. À l'aide de ces informations, l'ACFP peut bloquer temporairement les sessions client ou les adresses IP dont trop de tentatives ont échoué. AWS WAF effectue une inspection des réponses de manière asynchrone, afin de ne pas augmenter la latence de votre trafic Web.

> **Note**
>
> Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d'informations, consultez Tarification d'AWS WAF.

> **Note**
>
> La fonctionnalité ACFP n'est pas disponible pour les groupes d'utilisateurs Amazon Cognito.

Rubriques

AWS WAF Composants ACFP

Les principaux éléments de la prévention de AWS WAF la fraude (ACFP) lors de la création de comptes Fraud Control sont les suivants :

- **`AWSManagedRulesACFPRuleSet`**— Les règles de ce groupe de règles AWS gérées détectent, étiquettent et traitent différents types d'activités de création de comptes frauduleuses. Le groupe de règles inspecte les requêtes HTTP `GET` text/html que les clients envoient au point de terminaison d'enregistrement de compte spécifié et les demandes `POST` Web que les clients envoient au point de terminaison d'inscription de compte spécifié. Pour les CloudFront distributions protégées, le groupe de règles inspecte également les réponses que la distribution renvoie aux demandes de création de compte. Pour obtenir la liste des règles de ce groupe de règles, consultezAWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes. Vous incluez ce groupe de règles dans votre ACL Web à l'aide d'une déclaration de référence de groupe de règles géré. Pour plus d'informations sur l'utilisation de ce groupe de règles, consultezAjouter le groupe de règles géré par l'ACFP à votre ACL Web.

  > **Note**
  >
  > Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d’informations, consultez Tarification d’AWS WAF.

- Informations sur les pages d'enregistrement et de création de compte de votre application : vous devez fournir des informations sur les pages d'enregistrement et de création de votre compte

lorsque vous ajoutez le groupe de `AWSManagedRulesACFPRuleSet` règles à votre ACL Web. Cela permet au groupe de règles de restreindre la portée des demandes qu'il inspecte et de valider correctement les demandes Web de création de compte. La page d'inscription doit accepter les demandes `GET` texte/html. Le chemin de création du compte doit accepter les `POST` demandes. Le groupe de règles ACFP fonctionne avec les noms d'utilisateur au format e-mail. Pour plus d'informations, consultez Ajouter le groupe de règles géré par l'ACFP à votre ACL Web.

- Pour les CloudFront distributions protégées, détails sur la façon dont votre application répond aux tentatives de création de compte : vous fournissez des détails sur les réponses de votre application aux tentatives de création de compte, et le groupe de règles ACFP suit et gère les tentatives de création de comptes en masse à partir d'une seule adresse IP ou d'une seule session client. Pour plus d'informations sur la configuration de cette option, consultezAjouter le groupe de règles géré par l'ACFP à votre ACL Web.
- JavaScript et SDK d'intégration d'applications mobiles : implémentez AWS WAF JavaScript les SDK mobiles avec votre implémentation ACFP pour activer l'ensemble complet des fonctionnalités proposées par le groupe de règles. De nombreuses règles ACFP utilisent les informations fournies par les SDK pour la vérification des clients au niveau de la session et l'agrégation des comportements, nécessaires pour séparer le trafic client légitime du trafic des robots. Pour plus d'informations sur les kits SDK, consultez AWS WAF intégration d'applications clientes.

Vous pouvez combiner votre implémentation ACFP avec les éléments suivants pour vous aider à surveiller, régler et personnaliser vos protections.

- Journalisation et métriques : vous pouvez surveiller votre trafic et comprendre comment le groupe de règles géré par l'ACFP l'affecte, en configurant et en activant les journaux, la collecte de données Amazon Security Lake et CloudWatch les métriques Amazon pour votre ACL Web. Les étiquettes ajoutées `AWSManagedRulesACFPRuleSet` à vos requêtes Web sont incluses dans les données. Pour plus d'informations sur les optionsJournalisation AWS WAF du trafic ACL Web, consultezSurveillance avec Amazon CloudWatch, et Qu'est-ce qu'Amazon Security Lake ? .

  En fonction de vos besoins et du trafic que vous constatez, vous souhaiterez peut-être personnaliser votre `AWSManagedRulesACFPRuleSet` implémentation. Par exemple, vous souhaiterez peut-être exclure une partie du trafic de l'évaluation de l'ACFP ou modifier la façon dont il gère certaines tentatives de fraude liées à la création de comptes qu'il identifie, en utilisant des AWS WAF fonctionnalités telles que les déclarations de portée réduite ou les règles de correspondance des étiquettes.

- Étiquettes et règles de correspondance des étiquettes : pour toutes les règles `AWSManagedRulesACFPRuleSet` incluses, vous pouvez modifier le comportement de blocage pour qu'il soit comptabilisé, puis le comparer aux étiquettes ajoutées par les règles. Utilisez cette approche pour personnaliser la façon dont vous gérez les demandes Web identifiées par le groupe de règles géré par l'ACFP. Pour plus d'informations sur l'étiquetage et l'utilisation des instructions de correspondance des étiquettes, consultez Déclaration relative à la règle de correspondance des étiquettes etAWS WAF étiquettes sur les requêtes Web.
- Demandes et réponses personnalisées : vous pouvez ajouter des en-têtes personnalisés aux demandes que vous autorisez et vous pouvez envoyer des réponses personnalisées pour les demandes que vous bloquez. Pour ce faire, vous associez votre étiquette correspondante aux fonctionnalités de demande et de réponse AWS WAF personnalisées. Pour plus d'informations sur la personnalisation des demandes et des réponses, consultezDemandes et réponses Web personnalisées dans AWS WAF.

Pourquoi utiliser les SDK d'intégration d'applications avec ACFP

Nous vous recommandons vivement de mettre en œuvre les SDK d'intégration d'applications, afin d'utiliser le plus efficacement possible le groupe de règles ACFP.

- Fonctionnalité complète du groupe de règles : la règle ACFP `SignalClientHumanInteractivityAbsentLow` ne fonctionne qu'avec les jetons renseignés par les intégrations d'applications. Cette règle détecte et gère l'interactivité humaine anormale avec la page de l'application. Les SDK d'intégration des applications peuvent détecter l'interactivité humaine normale par le biais des mouvements de la souris, des pressions sur les touches et d'autres mesures. Les interstitiels envoyés par les règles agissent CAPTCHA et ne Challenge peuvent pas fournir ce type de données.
- Latence réduite : la règle du groupe de règles `AllRequests` applique l'action de la Challenge règle à toute demande ne comportant pas encore de jeton de défi. Dans ce cas, la demande est évaluée deux fois par le groupe de règles : une fois sans le jeton, puis une seconde fois après l'acquisition du jeton au moyen de l'Challengeaction interstitielle. Aucuns frais supplémentaires ne vous sont facturés pour la seule utilisation de la `AllRequests` règle, mais cette approche alourdit votre trafic Web et augmente la latence de votre expérience utilisateur final. Si vous acquérez le jeton côté client à l'aide des intégrations d'applications, le groupe de règles ACFP évalue la demande une fois avant d'envoyer la demande de création de compte.

Pour plus d'informations sur les fonctionnalités des groupes de règles, consultezAWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes.

Pour plus d'informations sur les SDK, consultezAWS WAF intégration d'applications clientes. Pour plus d'informations sur AWS WAF les jetons, consultezAWS WAF jetons de demande Web. Pour plus d'informations sur les actions des règles, consultezCAPTCHAet Challenge dans AWS WAF.

Ajouter le groupe de règles géré par l'ACFP à votre ACL Web

Pour configurer le groupe de règles géré par l'ACFP afin de reconnaître les activités frauduleuses liées à la création de compte dans votre trafic Web, vous fournissez des informations sur la manière dont les clients accèdent à votre page d'inscription et envoient des demandes de création de compte à votre application. Pour les CloudFront distributions Amazon protégées, vous fournissez également des informations sur la manière dont votre application répond aux demandes de création de compte. Cette configuration s'ajoute à la configuration normale d'un groupe de règles géré.

Pour la description du groupe de règles et la liste des règles, voirAWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes.

> **Note**
>
> La base de données d'identification volées de l'ACFP ne contient que des noms d'utilisateur au format e-mail.

Ce guide est destiné aux utilisateurs qui savent généralement comment créer et gérer des ACL, des règles et des groupes de règles AWS WAF Web. Ces sujets sont abordés dans les sections précédentes de ce guide. Pour obtenir des informations de base sur la façon d'ajouter un groupe de règles géré à votre ACL Web, consultezAjout d'un groupe de règles géré à une ACL Web via la console.

Suivez les meilleures pratiques

Utilisez le groupe de règles ACFP conformément aux meilleures pratiques deMeilleures pratiques pour une atténuation intelligente des menaces.

Pour utiliser le groupe de **`AWSManagedRulesACFPRuleSet`** règles dans votre ACL Web

1. Ajoutez le groupe de règles AWS géré `AWSManagedRulesACFPRuleSet` à votre ACL Web et modifiez les paramètres du groupe de règles avant de l'enregistrer.

   > **Note**
   >
   > Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d'informations, consultez Tarification d'AWS WAF.

2. Dans le volet de configuration du groupe de règles, fournissez les informations que le groupe de règles ACFP utilise pour inspecter les demandes de création de compte.

   a. Pour Utiliser une expression régulière dans les chemins, activez cette option si vous souhaitez effectuer une correspondance AWS WAF d'expressions régulières pour les spécifications du chemin de page d'enregistrement et de création de compte.

      AWS WAF prend en charge la syntaxe des modèles utilisée par la bibliothèque PCRE, `libpcre` à quelques exceptions près. La bibliothèque est documentée sur PCRE - Perl Compatible Regular Expressions. Pour plus d'informations sur AWS WAF le support, consultezModèle d'expression régulière correspondant dans AWS WAF.

   b. Pour le chemin de la page d'enregistrement, indiquez le chemin du point de terminaison de la page d'enregistrement de votre application. Cette page doit accepter les requêtes `GET` texte/html. Le groupe de règles inspecte uniquement les requêtes HTTP `GET` text/html adressées au point de terminaison de la page d'enregistrement que vous avez spécifiée.

      > **Note**
      >
      > La correspondance entre les points de terminaison ne fait pas la distinction majuscules/minuscules. Les spécifications Regex ne doivent pas contenir l'indicateur`(?-i)`, qui désactive la mise en correspondance indifférenciée des majuscules et minuscules. Les spécifications de chaîne doivent commencer par une barre oblique`/`.

      Par exemple, pour l'URL`https://example.com/web/registration`, vous pouvez fournir la spécification du chemin de chaîne`/web/registration`. Les chemins de page d'inscription qui commencent par le chemin que vous avez indiqué sont

considérés comme correspondants. Par exemple, `/web/registration` correspond aux chemins d'enregistrement `/web/registration` `/web/registration//web/registrationPage`,, et`/web/registration/thisPage`, mais ne correspond pas au chemin `/home/web/registration` ou`/website/registration`.

> **Note**
>
> Assurez-vous que vos utilisateurs finaux chargent la page d'inscription avant de soumettre une demande de création de compte. Cela permet de garantir que les demandes de création de compte émanant du client incluent des jetons valides.

c. Pour le chemin de création du compte, indiquez l'URI de votre site Web qui accepte les informations des nouveaux utilisateurs complétées. Cet URI doit accepter les `POST` demandes.

> **Note**
>
> La correspondance entre les points de terminaison ne fait pas la distinction majuscules/minuscules. Les spécifications Regex ne doivent pas contenir l'indicateur`(?-i)`, qui désactive la mise en correspondance indifférenciée des majuscules et minuscules. Les spécifications de chaîne doivent commencer par une barre oblique`/`.

Par exemple, pour l'URL`https://example.com/web/newaccount`, vous pouvez fournir la spécification du chemin de chaîne`/web/newaccount`. Les chemins de création de compte qui commencent par le chemin que vous avez indiqué sont considérés comme correspondants. Par exemple, `/web/newaccount` correspond aux chemins de création de compte `/web/newaccount` `/web/newaccount//web/newaccountPage`,, et`/web/newaccount/thisPage`, mais ne correspond pas au chemin `/home/web/newaccount` ou`/website/newaccount`.

d. Pour l'inspection des demandes, spécifiez comment votre application accepte les tentatives de création de compte en fournissant le type de charge utile de la demande et les noms des champs du corps de la demande dans lesquels le nom d'utilisateur, le mot de passe et les autres informations de création de compte sont fournis.

> **Note**
>
> Pour les champs d'adresse principale et de numéro de téléphone, indiquez les champs dans l'ordre dans lequel ils apparaissent dans la charge utile de la demande.

La spécification des noms de champs dépend du type de charge utile.

- Type de charge utile JSON — Spécifiez les noms des champs dans la syntaxe du pointeur JSON. Pour plus d'informations sur la syntaxe du pointeur JSON, consultez la documentation du pointeur JSON (JavaScriptObject Notation) de l'Internet Engineering Task Force (IETF).

  Par exemple, pour l'exemple de charge utile JSON suivant, la spécification du champ du nom d'utilisateur est `/signupform/username` et les spécifications du champ d'adresse principal sont `/signupform/addrp1`/`signupform/addrp2`, et`/signupform/addrp3`.

  ```
  {
      "signupform": {
          "username": "THE_USERNAME",
          "password": "THE_PASSWORD",
          "addrp1": "PRIMARY_ADDRESS_LINE_1",
          "addrp2": "PRIMARY_ADDRESS_LINE_2",
          "addrp3": "PRIMARY_ADDRESS_LINE_3",
          "phonepcode": "PRIMARY_PHONE_CODE",
          "phonepnumber": "PRIMARY_PHONE_NUMBER"
      }
  }
  ```

- Type de charge utile FORM_ENCODED — Utilisez les noms des formulaires HTML.

  Par exemple, pour un formulaire HTML dont les éléments de saisie d'utilisateur et de mot de passe sont nommés `username1` et`password1`, la spécification du champ du nom d'utilisateur est `username1` et celle du champ du mot de passe est`password1`.

e. Si vous protégez des CloudFront distributions Amazon, dans la section Inspection des réponses, précisez comment votre application indique le succès ou l'échec de ses réponses aux tentatives de création de compte.

> **Note**
>
> L'inspection des réponses ACFP n'est disponible que dans les ACL Web qui protègent CloudFront les distributions.

Spécifiez un seul composant dans la réponse de création de compte que vous souhaitez que l'ACFP inspecte. Pour les types de composants Body et JSON, AWS WAF vous pouvez inspecter les 65 536 premiers octets (64 Ko) du composant.

Indiquez vos critères d'inspection pour le type de composant, comme indiqué par l'interface. Vous devez fournir des critères de réussite et d'échec à inspecter dans le composant.

Supposons, par exemple, que votre application indique le statut d'une tentative de création de compte dans le code d'état de la réponse et qu'`200 OK`elle indique le succès `401 Unauthorized` et/ou `403 Forbidden` l'échec. Vous devez définir le type de composant d'inspection des réponses sur Code d'état, puis dans la zone de texte Succès, entrez `200` et dans la zone de texte Échec, entrez `401` sur la première ligne et `403` sur la seconde.

Le groupe de règles ACFP ne compte que les réponses correspondant à vos critères de réussite ou d'échec de l'inspection. Les règles des groupes de règles agissent sur les clients lorsque leur taux de réussite est trop élevé parmi les réponses prises en compte, afin de limiter les tentatives de création de comptes en masse. Pour respecter correctement les règles du groupe de règles, veillez à fournir des informations complètes sur les tentatives de création de compte réussies et infructueuses.

Pour voir les règles qui contrôlent les réponses relatives à la création de comptes, recherchez `VolumetricIPSuccessfulResponse` et `VolumetricSessionSuccessfulResponse` dans la liste des règles à l'adresse[AWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes](#).

3. Fournissez toute configuration supplémentaire que vous souhaitez pour le groupe de règles.

   Vous pouvez limiter davantage l'étendue des demandes inspectées par le groupe de règles en ajoutant une instruction scope-down à l'instruction du groupe de règles géré. Par exemple, vous ne pouvez inspecter que les demandes contenant un argument de requête ou un cookie spécifique. Le groupe de règles inspectera uniquement les demandes qui répondent aux critères

de votre déclaration de délimitation et qui sont envoyées aux chemins d'enregistrement et de création de compte que vous avez spécifiés dans la configuration du groupe de règles. Pour plus d'informations sur les instructions de portée réduite, consultez. Déclarations de portée réduite

4. Enregistrez les modifications apportées à l'ACL Web.

Avant de déployer votre implémentation ACFP pour le trafic de production, testez-la et ajustez-la dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite les règles en mode comptage avec votre trafic de production avant de les activer. Consultez la section qui suit pour obtenir des conseils.

Test et déploiement de l'ACFP

Cette section fournit des conseils généraux pour configurer et tester une implémentation de prévention de AWS WAF la fraude (ACFP) lors de la création de comptes Fraud Control pour votre site. Les étapes spécifiques que vous choisirez de suivre dépendront de vos besoins, des ressources et des demandes Web que vous recevrez.

Ces informations s'ajoutent aux informations générales sur les tests et le réglage fournies surTester et ajuster vos AWS WAF protections.

> **Note**
>
> AWS Les règles gérées sont conçues pour vous protéger contre les menaces Web les plus courantes. Lorsqu'ils sont utilisés conformément à la documentation, les groupes de règles AWS gérées ajoutent un niveau de sécurité supplémentaire à vos applications. Cependant, les groupes de règles AWS gérées ne sont pas destinés à remplacer vos responsabilités en matière de sécurité, qui sont déterminées par les AWS ressources que vous sélectionnez. Reportez-vous au modèle de responsabilité partagée pour vous assurer que vos ressources AWS sont correctement protégées.

> **Risque lié au trafic de production**
>
> Avant de déployer votre implémentation ACFP pour le trafic de production, testez-la et ajustez-la dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite les règles en mode comptage avec votre trafic de production avant de les activer.

AWS WAF fournit des informations d'identification de test que vous pouvez utiliser pour vérifier votre configuration ACFP. Dans la procédure suivante, vous allez configurer une ACL Web de test pour utiliser le groupe de règles géré par l'ACFP, configurer une règle pour capturer l'étiquette ajoutée par le groupe de règles, puis exécuter une tentative de création de compte à l'aide de ces informations d'identification de test. Vous allez vérifier que votre ACL Web a correctement géré la tentative en consultant les CloudWatch statistiques Amazon relatives à la tentative de création de compte.

Ce guide est destiné aux utilisateurs qui savent généralement comment créer et gérer des ACL, des règles et des groupes de règles AWS WAF Web. Ces sujets sont abordés dans les sections précédentes de ce guide.

Pour configurer et tester une implémentation de la prévention des AWS WAF fraudes (ACFP) lors de la création de comptes de contrôle des fraudes

Effectuez ces étapes d'abord dans un environnement de test, puis en production.

1. Ajouter le groupe de règles géré par AWS WAF Fraud Control pour la création de comptes et la prévention des fraudes (ACFP) en mode décompte

   > **Note**
   >
   > Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d'informations, consultez Tarification d'AWS WAF.

   Ajoutez le groupe de règles AWS gérées `AWSManagedRulesACFPRuleSet` à une ACL Web nouvelle ou existante et configurez-le de manière à ce qu'il ne modifie pas le comportement actuel de l'ACL Web. Pour plus de détails sur les règles et les libellés de ce groupe de règles, consultezAWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes.

   - Lorsque vous ajoutez le groupe de règles géré, modifiez-le et procédez comme suit :
     - Dans le volet de configuration du groupe de règles, fournissez les détails des pages d'enregistrement et de création de compte de votre application. Le groupe de règles ACFP utilise ces informations pour surveiller les activités de connexion. Pour plus d'informations, consultez Ajouter le groupe de règles géré par l'ACFP à votre ACL Web.
     - Dans le volet Règles, ouvrez le menu déroulant Remplacer toutes les actions des règles et choisissez. Count Avec cette configuration, AWS WAF évalue les demandes par rapport

à toutes les règles du groupe de règles et ne compte que les correspondances qui en résultent, tout en ajoutant des étiquettes aux demandes. Pour plus d'informations, consultez Remplacer les actions des règles dans un groupe de règles.

Grâce à cette dérogation, vous pouvez surveiller l'impact potentiel des règles gérées par l'ACFP afin de déterminer si vous souhaitez ajouter des exceptions, telles que des exceptions pour des cas d'utilisation internes.

- Positionnez le groupe de règles de manière à ce qu'il soit évalué selon vos règles existantes dans l'ACL Web, avec un paramètre de priorité numériquement supérieur à celui des règles ou groupes de règles que vous utilisez déjà. Pour plus d'informations, consultez Ordre de traitement des règles et des groupes de règles dans une ACL Web.

  De cette façon, votre gestion actuelle du trafic n'est pas perturbée. Par exemple, si vous avez des règles qui détectent le trafic malveillant tel que l'injection SQL ou les scripts intersites, elles continueront à le détecter et à le consigner. Par ailleurs, si vous avez des règles qui autorisent le trafic connu non malveillant, elles peuvent continuer à autoriser ce trafic, sans qu'il soit bloqué par le groupe de règles géré par l'ACFP. Vous pouvez décider d'ajuster l'ordre de traitement lors de vos activités de test et de réglage.

2. Implémenter les SDK d'intégration des applications

   Intégrez le AWS WAF JavaScript SDK dans les processus d'enregistrement et de création de compte de votre navigateur. AWS WAF fournit également des SDK mobiles pour intégrer les appareils iOS et Android. Pour plus d'informations sur les kits de développement logiciel (SDK) d'intégration, consultezAWS WAF intégration d'applications clientes. Pour plus d'informations sur cette recommandation, consultezPourquoi utiliser les SDK d'intégration d'applications avec ACFP.

   > **Note**
   >
   > Si vous ne parvenez pas à utiliser les SDK d'intégration d'applications, il est possible de tester le groupe de règles ACFP en le modifiant dans votre ACL Web et en supprimant la dérogation que vous avez accordée à la règle. `AllRequests` Cela active le paramètre Challenge d'action de la règle, afin de garantir que les demandes incluent un jeton de défi valide.
   > Faites-le d'abord dans un environnement de test, puis avec le plus grand soin dans votre environnement de production. Cette approche est susceptible de bloquer des utilisateurs. Par exemple, si le chemin de votre page d'inscription n'accepte pas les requêtes `GET`

texte/html, cette configuration de règles peut bloquer efficacement toutes les demandes sur la page d'enregistrement.

3. Activer la journalisation et les métriques pour l'ACL Web

   Le cas échéant, configurez la journalisation, la collecte de données Amazon Security Lake, l'échantillonnage des demandes et CloudWatch les métriques Amazon pour l'ACL Web. Vous pouvez utiliser ces outils de visibilité pour surveiller l'interaction du groupe de règles géré par l'ACFP avec votre trafic.

   - Pour de plus amples informations sur la journalisation, veuillez consulter Journalisation AWS WAF du trafic ACL Web.
   - Pour plus d'informations sur Amazon Security Lake, consultez Qu'est-ce qu'Amazon Security Lake ? et Collecte de données à partir AWS des services décrits dans le guide de l'utilisateur d'Amazon Security Lake.
   - Pour plus d'informations sur CloudWatch les métriques Amazon, consultezSurveillance avec Amazon CloudWatch.
   - Pour plus d'informations sur l'échantillonnage des requêtes Web, consultezAffichage d'un exemple de demandes web.

4. Associer l'ACL Web à une ressource

   Si l'ACL Web n'est pas déjà associée à une ressource de test, associez-la. Pour plus d'informations, veuillez consulter Associer ou dissocier une ACL Web à une ressource AWS.

5. Surveillez le trafic et les correspondances aux règles ACFP

   Assurez-vous que votre trafic normal circule et que les règles du groupe de règles géré par l'ACFP ajoutent des étiquettes aux requêtes Web correspondantes. Vous pouvez voir les étiquettes dans les journaux, ainsi que l'ACFP et les métriques relatives aux étiquettes dans les CloudWatch métriques Amazon. Dans les journaux, les règles que vous avez remplacées pour être prises en compte dans le groupe de règles apparaissent dans le `ruleGroupList` champ « `action` set to count » et `overriddenAction` indiquent l'action de règle configurée que vous avez remplacée.

6. Testez les capacités de vérification des informations d'identification du groupe de règles

   Effectuez une tentative de création de compte en testant les informations d'identification compromises et vérifiez que le groupe de règles correspond à celles-ci, comme prévu.

a. Accédez à la page d'enregistrement du compte de votre ressource protégée et essayez d'ajouter un nouveau compte. Utilisez la paire d'identifiants de AWS WAF test suivante et participez à n'importe quel test

   - Utilisateur : `WAF_TEST_CREDENTIAL@wafexample.com`
   - Mot de passe : `WAF_TEST_CREDENTIAL_PASSWORD`

   Ces informations d'identification de test sont classées dans la catégorie des informations d'identification compromises, et le groupe de règles géré par l'ACFP ajoutera l'`awswaf:managed:aws:acfp:signal:credential_compromised`étiquette à la demande de création de compte, que vous pouvez consulter dans les journaux.

b. Dans vos journaux ACL Web, recherchez l'`awswaf:managed:aws:acfp:signal:credential_compromised`étiquette dans le `labels` champ des entrées du journal pour votre demande de création de compte de test. Pour de plus amples informations sur la journalisation, veuillez consulter Journalisation AWS WAF du trafic ACL Web.

Après avoir vérifié que le groupe de règles capture les informations d'identification compromises comme prévu, vous pouvez prendre des mesures pour configurer sa mise en œuvre en fonction de vos besoins pour votre ressource protégée.

7. Pour les CloudFront distributions, testez la gestion par le groupe de règles des tentatives de création de comptes en masse

   Exécutez ce test pour chaque critère de réponse positive que vous avez configuré pour le groupe de règles ACFP. Attendez au moins 30 minutes entre les tests.

   a. Pour chacun de vos critères de succès, identifiez une tentative de création de compte qui sera couronnée de succès avec ce critère de succès dans la réponse. Ensuite, à partir d'une seule session client, effectuez au moins 5 tentatives de création de compte réussies en moins de 30 minutes. Un utilisateur ne crée normalement qu'un seul compte sur votre site.

      Une fois la première création de compte réussie, la `VolumetricSessionSuccessfulResponse` règle devrait commencer à correspondre aux autres réponses à la création de votre compte, à les étiqueter et à les compter, en fonction de votre dérogation à l'action de la règle. Il se peut que la règle omette le premier ou les deux premiers en raison de la latence.

b. Dans vos journaux ACL Web, recherchez l'`awswaf:managed:aws:acfp:aggregate:volumetric:session:successful_creation_` dans le `labels` champ des entrées du journal pour vos demandes Web de création de compte de test. Pour de plus amples informations sur la journalisation, veuillez consulter Journalisation AWS WAF du trafic ACL Web.

Ces tests vérifient que vos critères de réussite correspondent à vos réponses en vérifiant que le nombre de réussites agrégés par la règle dépasse le seuil de la règle. Une fois le seuil atteint, si vous continuez à envoyer des demandes de création de compte depuis la même session, la règle continuera de correspondre jusqu'à ce que le taux de réussite tombe en dessous du seuil. Lorsque le seuil est dépassé, la règle fait correspondre les tentatives de création de compte réussies ou non à partir de l'adresse de session.

8. Personnaliser le traitement des requêtes Web ACFP

   Le cas échéant, ajoutez vos propres règles qui autorisent ou bloquent explicitement les demandes, afin de modifier la façon dont les règles ACFP les traiteraient autrement.

   Par exemple, vous pouvez utiliser les étiquettes ACFP pour autoriser ou bloquer les demandes ou pour personnaliser le traitement des demandes. Vous pouvez ajouter une règle de correspondance d'étiquettes après le groupe de règles géré par l'ACFP afin de filtrer les demandes étiquetées pour le traitement que vous souhaitez appliquer. Après le test, maintenez les règles ACFP associées en mode décompte et conservez les décisions relatives au traitement des demandes dans votre règle personnalisée. Pour obtenir un exemple, consultez Exemple ACFP : réponse personnalisée pour des informations d'identification compromises.

9. Supprimez vos règles de test et activez les paramètres du groupe de règles géré par l'ACFP

   Selon votre situation, vous avez peut-être décidé de laisser certaines règles ACFP en mode décompte. Pour les règles que vous souhaitez exécuter telles que configurées au sein du groupe de règles, désactivez le mode de comptage dans la configuration du groupe de règles ACL Web. Lorsque vous avez terminé le test, vous pouvez également supprimer les règles de correspondance de vos étiquettes de test.

10. Surveillez et réglez

    Pour vous assurer que les requêtes Web sont traitées comme vous le souhaitez, surveillez attentivement votre trafic après avoir activé la fonctionnalité ACFP que vous souhaitez utiliser. Ajustez le comportement selon vos besoins en annulant le nombre de règles sur le groupe de règles et en appliquant vos propres règles.

Une fois que vous avez terminé de tester l'implémentation de votre groupe de règles ACFP, si vous n'avez pas encore intégré le AWS WAF JavaScript SDK dans les pages d'enregistrement et de création de compte de votre navigateur, nous vous recommandons vivement de le faire. AWS WAF fournit également des SDK mobiles pour intégrer les appareils iOS et Android. Pour plus d'informations sur les kits de développement logiciel (SDK) d'intégration, consultezAWS WAF intégration d'applications clientes. Pour plus d'informations sur cette recommandation, consultezPourquoi utiliser les SDK d'intégration d'applications avec ACFP.

AWS WAF Exemples de création de comptes Fraud Control et de prévention de la fraude (ACFP)

Cette section présente des exemples de configurations qui répondent aux cas d'utilisation courants pour les implémentations de création de comptes AWS WAF Fraud Control et de prévention de la fraude (ACFP).

Chaque exemple fournit une description du cas d'utilisation, puis montre la solution dans les listes JSON pour les règles configurées personnalisées.

> **Note**
>
> Vous pouvez récupérer des listes JSON telles que celles présentées dans ces exemples via le téléchargement ACL JSON sur la console Web ou l'éditeur JSON de règles, ou via les `getWebACL` opérations dans les API et l'interface de ligne de commande.

Rubriques

- Exemple ACFP : configuration simple
- Exemple ACFP : réponse personnalisée pour des informations d'identification compromises
- Exemple ACFP : configuration de l'inspection des réponses

Exemple ACFP : configuration simple

La liste JSON suivante montre un exemple d'ACL Web avec un groupe de règles géré par AWS WAF Fraud Control pour la création de comptes et la prévention des fraudes (ACFP). Notez les `RegistrationPagePath` configurations supplémentaires`CreationPath`, ainsi que le type de charge utile et les informations nécessaires pour localiser les nouvelles informations de compte dans la charge utile, afin de les vérifier. Le groupe de règles utilise ces informations pour surveiller et gérer

vos demandes de création de compte. Ce JSON inclut les paramètres générés automatiquement par l'ACL Web, tels que l'espace de noms des étiquettes et l'URL d'intégration de l'application de l'ACL Web.

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    },
```

```
                    {
                      "Identifier": "/form/phonenumber"
                    }
                  ],
                  "AddressFields": [
                    {
                      "Identifier": "/form/name"
                    },
                    {
                      "Identifier": "/form/street-address"
                    },
                    {
                      "Identifier": "/form/city"
                    },
                    {
                      "Identifier": "/form/state"
                    },
                    {
                      "Identifier": "/form/zipcode"
                    }
                  ]
                },
                "EnableRegexInPath": false
              }
            }
          ]
        }
      },
      "OverrideAction": {
        "None": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "simpleACFP"
  },
  "Capacity": 50,
```

```
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
}
```

Exemple ACFP : réponse personnalisée pour des informations d'identification compromises

Par défaut, la vérification des informations d'identification effectuée par le groupe de règles `AWSManagedRulesACFPRuleSet` traite les informations d'identification compromises en étiquetant la demande et en la bloquant. Pour plus de détails sur le groupe de règles et le comportement des règles, consultezAWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes.

Pour informer l'utilisateur que les informations d'identification du compte qu'il a fournies ont été compromises, vous pouvez procéder comme suit :

- Remplacer la **`SignalCredentialCompromised`** règle par Count : la règle ne compte et n'étiquette que les demandes correspondantes.
- Ajouter une règle de correspondance des étiquettes avec gestion personnalisée : configurez cette règle pour qu'elle corresponde à l'étiquette ACFP et pour effectuer votre gestion personnalisée.

Les listes d'ACL Web suivantes montrent le groupe de règles géré par l'ACFP dans l'exemple précédent, l'action de la `SignalCredentialCompromised` règle étant remplacée pour compter. Avec cette configuration, lorsque ce groupe de règles évalue une demande Web utilisant des informations d'identification compromises, il étiquette la demande, mais ne la bloque pas.

En outre, l'ACL Web possède désormais une réponse personnalisée nommée `aws-waf-credential-compromised` et une nouvelle règle nomméeAccountSignupCompromisedCredentialsHandling. La priorité de la règle est un paramètre numérique supérieur à celui du groupe de règles. Elle s'exécute donc après le groupe de règles dans l'évaluation de l'ACL Web. La nouvelle règle associe toutes les demandes à l'étiquette d'identification compromise du groupe de règles. Lorsque la règle trouve une correspondance, elle applique l'Blockaction à la demande avec le corps de réponse personnalisé. Le corps de réponse personnalisé indique à l'utilisateur final que ses informations d'identification ont été compromises et propose une action à entreprendre.

```
{
  "Name": "compromisedCreds",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/compromisedCreds/...",
```

```
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
                  },
                  "PasswordField": {
                    "Identifier": "/form/password"
                  },
                  "EmailField": {
                    "Identifier": "/form/email"
                  },
                  "PhoneNumberFields": [
                    {
                      "Identifier": "/form/country-code"
                    },
                    {
                      "Identifier": "/form/region-code"
                    },
                    {
                      "Identifier": "/form/phonenumber"
                    }
                  ],
                  "AddressFields": [
                    {
                      "Identifier": "/form/name"
                    },
                    {
```

```
                    "Identifier": "/form/street-address"
                  },
                  {
                    "Identifier": "/form/city"
                  },
                  {
                    "Identifier": "/form/state"
                  },
                  {
                    "Identifier": "/form/zipcode"
                  }
                ]
              },
              "EnableRegexInPath": false
            }
          }
        ],
        "RuleActionOverrides": [
          {
            "Name": "SignalCredentialCompromised",
            "ActionToUse": {
              "Count": {}
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
    }
  },
  {
    "Name": "AccountSignupCompromisedCredentialsHandling",
    "Priority": 1,
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:acfp:signal:credential_compromised"
      }
```

```
      },
      "Action": {
        "Block": {
          "CustomResponse": {
            "ResponseCode": 406,
            "CustomResponseBodyKey": "aws-waf-credential-compromised",
            "ResponseHeaders": [
              {
                "Name": "aws-waf-credential-compromised",
                "Value": "true"
              }
            ]
          }
        }
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "AccountSignupCompromisedCredentialsHandling"
      }
    }
  ],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "compromisedCreds"
  },
  "Capacity": 51,
  "ManagedByFirewallManager": false,
  "LabelNamespace": "awswaf:111122223333:webacl:compromisedCreds:",
  "CustomResponseBodies": {
    "aws-waf-credential-compromised": {
      "ContentType": "APPLICATION_JSON",
      "Content": "{\n  \"credentials-compromised\": \"The credentials you provided have
 been found in a compromised credentials database.\\n\\nTry again with a different
 username, password pair.\"\n}"
    }
  }
}
```

Exemple ACFP : configuration de l'inspection des réponses

La liste JSON suivante montre un exemple d'ACL Web avec un AWS WAF groupe de règles géré par Fraud Control pour la création de comptes et la prévention des fraudes (ACFP) configuré pour inspecter les réponses d'origine. Notez la configuration de l'inspection des réponses, qui spécifie les codes de réussite et d'état de réponse. Vous pouvez également configurer les paramètres de réussite et de réponse en fonction des correspondances JSON entre en-tête, corps et corps. Ce JSON inclut les paramètres générés automatiquement par l'ACL Web, tels que l'espace de noms des étiquettes et l'URL d'intégration de l'application de l'ACL Web.

> **Note**
>
> L'inspection des réponses ATP n'est disponible que dans les ACL Web qui protègent les CloudFront distributions.

```
{
  "Name": "simpleACFP",
  "Id": "... ",
  "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/simpleACFP/... ",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "",
  "Rules": [
    {
      "Name": "AWS-AWSManagedRulesACFPRuleSet",
      "Priority": 0,
      "Statement": {
        "ManagedRuleGroupStatement": {
          "VendorName": "AWS",
          "Name": "AWSManagedRulesACFPRuleSet",
          "ManagedRuleGroupConfigs": [
            {
              "AWSManagedRulesACFPRuleSet": {
                "CreationPath": "/web/signup/submit-registration",
                "RegistrationPagePath": "/web/signup/registration",
                "RequestInspection": {
                  "PayloadType": "JSON",
                  "UsernameField": {
                    "Identifier": "/form/username"
```

```
      },
      "PasswordField": {
        "Identifier": "/form/password"
      },
      "EmailField": {
        "Identifier": "/form/email"
      },
      "PhoneNumberFields": [
        {
          "Identifier": "/form/country-code"
        },
        {
          "Identifier": "/form/region-code"
        },
        {
          "Identifier": "/form/phonenumber"
        }
      ],
      "AddressFields": [
        {
          "Identifier": "/form/name"
        },
        {
          "Identifier": "/form/street-address"
        },
        {
          "Identifier": "/form/city"
        },
        {
          "Identifier": "/form/state"
        },
        {
          "Identifier": "/form/zipcode"
        }
      ]
    },
    "ResponseInspection": {
      "StatusCode": {
        "SuccessCodes": [
          200
        ],
        "FailureCodes": [
          401
        ]
```

```
                }
              },
              "EnableRegexInPath": false
            }
          }
        ]
      }
    },
    "OverrideAction": {
      "None": {}
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSManagedRulesACFPRuleSet"
    }
  }
],
"VisibilityConfig": {
  "SampledRequestsEnabled": true,
  "CloudWatchMetricsEnabled": true,
  "MetricName": "simpleACFP"
},
"Capacity": 50,
"ManagedByFirewallManager": false,
"LabelNamespace": "awswaf:111122223333:webacl:simpleACFP:"
}
```

AWS WAF Contrôle des fraudes et prévention des prises de contrôle des comptes (ATP)

Le piratage de compte est une activité illégale en ligne au cours de laquelle un attaquant obtient un accès non autorisé au compte d'une personne. L'attaquant peut le faire de différentes manières, par exemple en utilisant des informations d'identification volées ou en devinant le mot de passe de la victime au cours d'une série de tentatives. Lorsque l'attaquant y accède, il peut voler de l'argent, des informations ou des services à la victime. L'attaquant peut se faire passer pour la victime pour accéder à d'autres comptes qu'elle possède ou pour accéder aux comptes d'autres personnes ou organisations. En outre, ils peuvent tenter de modifier le mot de passe de l'utilisateur afin de bloquer l'accès de la victime à ses propres comptes.

Vous pouvez surveiller et contrôler les tentatives de prise de contrôle de compte en mettant en œuvre la fonction de prévention du piratage de compte AWS WAF Fraud Control (ATP). AWS WAF propose cette fonctionnalité dans le groupe de règles AWS Managed Rules `AWSManagedRulesATPRuleSet` et dans les SDK d'intégration d'applications associés.

Le groupe de règles géré par ATP étiquette et gère les demandes susceptibles de faire partie de tentatives malveillantes de prise de contrôle de compte. Pour ce faire, le groupe de règles inspecte les tentatives de connexion que les clients envoient au point de terminaison de connexion de votre application.

- Inspection des demandes — ATP vous donne de la visibilité et un contrôle sur les tentatives de connexion anormales et les tentatives de connexion utilisant des informations d'identification volées, afin d'empêcher les prises de contrôle de comptes susceptibles de mener à des activités frauduleuses. ATP vérifie les combinaisons d'e-mails et de mots de passe par rapport à sa base de données d'identifiants volés, qui est régulièrement mise à jour à mesure que de nouvelles informations d'identification divulguées sont découvertes sur le Dark Web. ATP agrège les données par adresse IP et par session client, afin de détecter et de bloquer les clients qui envoient trop de demandes suspectes.
- Inspection des réponses — Pour les CloudFront distributions, en plus d'inspecter les demandes de connexion entrantes, le groupe de règles ATP inspecte les réponses de votre application aux tentatives de connexion, afin de suivre les taux de réussite et d'échec. À l'aide de ces informations, ATP peut bloquer temporairement les sessions client ou les adresses IP présentant trop d'échecs de connexion. AWS WAF effectue une inspection des réponses de manière asynchrone, afin de ne pas augmenter la latence de votre trafic Web.

> **Note**
>
> Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d'informations, consultez Tarification d'AWS WAF.

> **Note**
>
> La fonctionnalité ATP n'est pas disponible pour les groupes d'utilisateurs Amazon Cognito.

Rubriques

- AWS WAF Composants ATP
- Pourquoi utiliser les SDK d'intégration d'applications avec ATP
- Ajouter le groupe de règles géré par ATP à votre ACL Web
- Tester et déployer ATP
- AWS WAF Exemples de prévention des prises de contrôle des fraudes (ATP)

AWS WAF Composants ATP

Les principaux éléments de la prévention des prises de contrôle des AWS WAF fraudes (ATP) sont les suivants :

- **`AWSManagedRulesATPRuleSet`**— Les règles de ce groupe de règles AWS gérées détectent, étiquettent et gèrent différents types d'activités de prise de contrôle de compte. Le groupe de règles inspecte les requêtes `POST` Web HTTP que les clients envoient au point de terminaison de connexion spécifié. Pour les CloudFront distributions protégées, le groupe de règles inspecte également les réponses que la distribution renvoie à ces demandes. Pour obtenir la liste des règles du groupe de règles, consultezAWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP). Vous incluez ce groupe de règles dans votre ACL Web à l'aide d'une déclaration de référence de groupe de règles géré. Pour plus d'informations sur l'utilisation de ce groupe de règles, consultezAjouter le groupe de règles géré par ATP à votre ACL Web.

  > **Note**
  >
  > Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d’informations, consultez Tarification d’AWS WAF.

- Informations sur la page de connexion de votre application : vous devez fournir des informations sur votre page de connexion lorsque vous ajoutez le groupe de `AWSManagedRulesATPRuleSet` règles à votre ACL Web. Cela permet au groupe de règles de restreindre l'étendue des demandes qu'il inspecte et de valider correctement l'utilisation des informations d'identification dans les requêtes Web. Le groupe de règles ATP fonctionne avec les noms d'utilisateur au format e-mail. Pour plus d’informations, consultez Ajouter le groupe de règles géré par ATP à votre ACL Web.
- Pour les CloudFront distributions protégées, détails sur la façon dont votre application répond aux tentatives de connexion : vous fournissez des informations sur les réponses de votre application aux tentatives de connexion, et le groupe de règles suit et gère les clients qui envoient trop de

tentatives de connexion infructueuses. Pour plus d'informations sur la configuration de cette option, consultezAjouter le groupe de règles géré par ATP à votre ACL Web.

- JavaScript et SDK d'intégration d'applications mobiles : implémentez les SDK mobiles AWS WAF JavaScript et les SDK mobiles avec votre implémentation ATP pour activer l'ensemble complet des fonctionnalités proposées par le groupe de règles. De nombreuses règles ATP utilisent les informations fournies par les SDK pour la vérification des clients au niveau de la session et l'agrégation des comportements, nécessaires pour séparer le trafic client légitime du trafic des robots. Pour plus d'informations sur les kits SDK, consultez AWS WAF intégration d'applications clientes.

Vous pouvez combiner votre implémentation ATP avec les éléments suivants pour vous aider à surveiller, régler et personnaliser vos protections.

- Journalisation et métriques : vous pouvez surveiller votre trafic et comprendre comment le groupe de règles géré par l'ACFP l'affecte, en configurant et en activant les journaux, la collecte de données Amazon Security Lake et CloudWatch les métriques Amazon pour votre ACL Web. Les étiquettes ajoutées `AWSManagedRulesATPRuleSet` à vos requêtes Web sont incluses dans les données. Pour plus d'informations sur les optionsJournalisation AWS WAF du trafic ACL Web, consultezSurveillance avec Amazon CloudWatch, et Qu'est-ce qu'Amazon Security Lake ? .

  En fonction de vos besoins et du trafic que vous constatez, vous souhaiterez peut-être personnaliser votre `AWSManagedRulesATPRuleSet` implémentation. Par exemple, vous souhaiterez peut-être exclure une partie du trafic de l'évaluation ATP ou modifier la façon dont elle gère certaines tentatives de prise de contrôle de compte qu'elle identifie, en utilisant des AWS WAF fonctionnalités telles que les instructions de portée réduite ou les règles de correspondance des étiquettes.
- Étiquettes et règles de correspondance des étiquettes : pour toutes les règles `AWSManagedRulesATPRuleSet` incluses, vous pouvez modifier le comportement de blocage pour qu'il soit comptabilisé, puis le comparer aux étiquettes ajoutées par les règles. Utilisez cette approche pour personnaliser la façon dont vous gérez les demandes Web identifiées par le groupe de règles géré par ATP. Pour plus d'informations sur l'étiquetage et l'utilisation des instructions de correspondance des étiquettes, consultez Déclaration relative à la règle de correspondance des étiquettes etAWS WAF étiquettes sur les requêtes Web.
- Demandes et réponses personnalisées : vous pouvez ajouter des en-têtes personnalisés aux demandes que vous autorisez et vous pouvez envoyer des réponses personnalisées pour les demandes que vous bloquez. Pour ce faire, vous associez votre étiquette correspondante aux

fonctionnalités de demande et de réponse AWS WAF personnalisées. Pour plus d'informations sur la personnalisation des demandes et des réponses, consultezDemandes et réponses Web personnalisées dans AWS WAF.

Pourquoi utiliser les SDK d'intégration d'applications avec ATP

Le groupe de règles géré par ATP nécessite les jetons de défi générés par les SDK d'intégration d'applications. Les jetons activent l'ensemble complet des protections proposées par le groupe de règles.

Nous vous recommandons vivement de mettre en œuvre les SDK d'intégration d'applications, afin d'utiliser le plus efficacement possible le groupe de règles ATP. Le script de défi doit être exécuté avant le groupe de règles ATP pour que celui-ci puisse bénéficier des jetons acquis par le script. Cela se produit automatiquement avec les SDK d'intégration des applications. Si vous ne parvenez pas à utiliser les SDK, vous pouvez également configurer votre ACL Web afin qu'elle exécute l'action de CAPTCHA règle Challenge ou contre toutes les demandes qui seront inspectées par le groupe de règles ATP. L'utilisation de l'action Challenge ou de la CAPTCHA règle peut entraîner des frais supplémentaires. Pour plus d'informations sur la tarification, consultez la page AWS WAF Pricing (Tarification).

Fonctionnalités du groupe de règles ATP ne nécessitant pas de jeton

Lorsque les requêtes Web ne comportent pas de jeton, le groupe de règles géré par ATP est capable de bloquer les types de trafic suivants :

- Adresses IP uniques qui font de nombreuses demandes de connexion.
- Des adresses IP uniques qui font de nombreuses demandes de connexion infructueuses en peu de temps.
- Tentatives de connexion avec traversée de mots de passe, en utilisant le même nom d'utilisateur mais en modifiant les mots de passe.

Fonctionnalités du groupe de règles ATP nécessitant un jeton

Les informations fournies dans le jeton de défi étendent les capacités du groupe de règles et améliorent la sécurité globale de vos applications clientes.

Le jeton fournit des informations sur le client à chaque demande Web, ce qui permet au groupe de règles ATP de séparer les sessions client légitimes des sessions client mal gérées, même lorsque les

deux proviennent d'une seule adresse IP. Le groupe de règles utilise les informations contenues dans les jetons pour agréger le comportement des demandes de session client afin d'affiner la détection et l'atténuation.

Lorsque le jeton est disponible dans les requêtes Web, le groupe de règles ATP peut détecter et bloquer les catégories supplémentaires de clients suivantes au niveau de la session :

- Sessions client qui échouent au défi silencieux géré par les SDK.
- Sessions client qui utilisent des noms d'utilisateur ou des mots de passe. C'est ce que l'on appelle également le credential stuffing.
- Sessions clientes qui utilisent à plusieurs reprises des informations d'identification volées pour se connecter.
- Sessions client qui passent beaucoup de temps à essayer de se connecter.
- Sessions clients qui font de nombreuses demandes de connexion. Le groupe de règles ATP permet une meilleure isolation des clients que la règle AWS WAF basée sur le taux, qui peut bloquer les clients par adresse IP. Le groupe de règles ATP utilise également un seuil inférieur.
- Sessions clients qui font de nombreuses demandes de connexion infructueuses en peu de temps. Cette fonctionnalité est disponible pour les CloudFront distributions Amazon protégées.

Pour plus d'informations sur les fonctionnalités des groupes de règles, consultezAWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP).

Pour plus d'informations sur les SDK, consultezAWS WAF intégration d'applications clientes. Pour plus d'informations sur AWS WAF les jetons, consultezAWS WAF jetons de demande Web. Pour plus d'informations sur les actions des règles, consultezCAPTCHAet Challenge dans AWS WAF.

Ajouter le groupe de règles géré par ATP à votre ACL Web

Pour configurer le groupe de règles géré par ATP afin de reconnaître les activités de prise de contrôle de compte dans votre trafic Web, vous fournissez des informations sur la manière dont les clients envoient des demandes de connexion à votre application. Pour les CloudFront distributions Amazon protégées, vous fournissez également des informations sur la manière dont votre application répond aux demandes de connexion. Cette configuration s'ajoute à la configuration normale d'un groupe de règles géré.

Pour la description du groupe de règles et la liste des règles, voirAWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP).

> **Note**
>
> La base de données d'identification volées ATP ne contient que des noms d'utilisateur au format e-mail.

Ce guide est destiné aux utilisateurs qui savent généralement comment créer et gérer des ACL, des règles et des groupes de règles AWS WAF Web. Ces sujets sont abordés dans les sections précédentes de ce guide. Pour obtenir des informations de base sur la façon d'ajouter un groupe de règles géré à votre ACL Web, consultezAjout d'un groupe de règles géré à une ACL Web via la console.

Suivez les meilleures pratiques

Utilisez le groupe de règles ATP conformément aux meilleures pratiques deMeilleures pratiques pour une atténuation intelligente des menaces.

Pour utiliser le groupe de **`AWSManagedRulesATPRuleSet`** règles dans votre ACL Web

1. Ajoutez le groupe de règles AWS géré `AWSManagedRulesATPRuleSet` à votre ACL Web et modifiez les paramètres du groupe de règles avant de l'enregistrer.

   > **Note**
   >
   > Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d'informations, consultez Tarification d'AWS WAF.

2. Dans le volet de configuration du groupe de règles, fournissez les informations que le groupe de règles ATP utilise pour inspecter les demandes de connexion.

   a. Pour Utiliser une expression régulière dans les chemins, activez cette option si vous souhaitez effectuer une correspondance AWS WAF d'expressions régulières pour les spécifications du chemin de votre page de connexion.

      AWS WAF prend en charge la syntaxe des modèles utilisée par la bibliothèque PCRE, `libpcre` à quelques exceptions près. La bibliothèque est documentée sur PCRE - Perl Compatible Regular Expressions. Pour plus d'informations sur AWS WAF le support, consultezModèle d'expression régulière correspondant dans AWS WAF.

b. Pour le chemin de connexion, indiquez le chemin du point de terminaison de connexion de votre application. Le groupe de règles inspecte uniquement les `POST` requêtes HTTP adressées au point de connexion que vous avez spécifié.

> **Note**
>
> La correspondance entre les points de terminaison ne fait pas la distinction majuscules/minuscules. Les spécifications Regex ne doivent pas contenir l'indicateur`(?-i)`, qui désactive la mise en correspondance insensible aux majuscules et minuscules. Les spécifications de chaîne doivent commencer par une barre oblique`/`.

Par exemple, pour l'URL`https://example.com/web/login`, vous pouvez fournir la spécification du chemin de chaîne`/web/login`. Les chemins de connexion qui commencent par le chemin que vous avez indiqué sont considérés comme correspondants. Par exemple, `/web/login` correspond aux chemins de connexion `/web/login/web/login/`,`/web/loginPage`, et`/web/login/thisPage`, mais ne correspond pas au chemin de connexion `/home/web/login` ou`/website/login`.

c. Pour l'inspection des demandes, spécifiez comment votre application accepte les tentatives de connexion en fournissant le type de charge utile de la demande et les noms des champs du corps de la demande où le nom d'utilisateur et le mot de passe sont fournis. La spécification des noms de champs dépend du type de charge utile.

- Type de charge utile JSON — Spécifiez les noms des champs dans la syntaxe du pointeur JSON. Pour plus d'informations sur la syntaxe du pointeur JSON, consultez la documentation du pointeur JSON (JavaScriptObject Notation) de l'Internet Engineering Task Force (IETF).

  Par exemple, pour l'exemple de charge utile JSON suivant, la spécification du champ du nom d'utilisateur est `/login/username` et la spécification du champ du mot de passe est`/login/password`.

```
{
    "login": {
        "username": "THE_USERNAME",
        "password": "THE_PASSWORD"
    }
```

```
}
```

- Type de charge utile FORM_ENCODED — Utilisez les noms des formulaires HTML.

  Par exemple, pour un formulaire HTML dont les éléments d'entrée sont nommés `username1` et`password1`, la spécification du champ du nom d'utilisateur est `username1` et celle du champ du mot de passe est`password1`.

d. Si vous protégez des CloudFront distributions Amazon, dans la section Inspection des réponses, spécifiez comment votre application indique le succès ou l'échec dans ses réponses aux tentatives de connexion.

> **Note**
>
> L'inspection des réponses ATP n'est disponible que dans les ACL Web qui protègent les CloudFront distributions.

Spécifiez un seul composant dans la réponse de connexion que vous souhaitez qu'ATP inspecte. Pour les types de composants Body et JSON, AWS WAF vous pouvez inspecter les 65 536 premiers octets (64 Ko) du composant.

Indiquez vos critères d'inspection pour le type de composant, comme indiqué par l'interface. Vous devez fournir des critères de réussite et d'échec à inspecter dans le composant.

Supposons, par exemple, que votre application indique l'état d'une tentative de connexion dans le code d'état de la réponse, et qu'elle l'utilise `200 OK` en cas de réussite `401 Unauthorized` et/ou `403 Forbidden` d'échec. Vous devez définir le type de composant d'inspection des réponses sur Code d'état, puis dans la zone de texte Succès, entrez `200` et dans la zone de texte Échec, entrez `401` sur la première ligne et `403` sur la seconde.

Le groupe de règles ATP ne compte que les réponses correspondant à vos critères de réussite ou d'échec de l'inspection. Les règles du groupe de règles agissent sur les clients alors que leur taux d'échec est trop élevé parmi les réponses prises en compte. Pour que les règles du groupe de règles se comportent correctement, veillez à fournir des informations complètes sur les tentatives de connexion réussies et échouées.

Pour voir les règles qui inspectent les réponses de connexion, recherchez `VolumetricIpFailedLoginResponseHigh` et `VolumetricSessionFailedLoginResponseHigh` dans la liste des règles à

l'adresseAWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP).

3. Fournissez toute configuration supplémentaire que vous souhaitez pour le groupe de règles.

   Vous pouvez limiter davantage l'étendue des demandes inspectées par le groupe de règles en ajoutant une instruction scope-down à l'instruction du groupe de règles géré. Par exemple, vous ne pouvez inspecter que les demandes contenant un argument de requête ou un cookie spécifique. Le groupe de règles inspectera uniquement les `POST` requêtes HTTP adressées au point de connexion que vous avez spécifié et qui répondent aux critères de votre instruction scope-down. Pour plus d'informations sur les instructions de portée réduite, voir. Déclarations de portée réduite

4. Enregistrez les modifications apportées à l'ACL Web.

Avant de déployer votre implémentation ATP pour le trafic de production, testez-la et ajustez-la dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite les règles en mode comptage avec votre trafic de production avant de les activer. Consultez la section qui suit pour obtenir des conseils.

Tester et déployer ATP

Cette section fournit des conseils généraux pour configurer et tester une implémentation de prévention du piratage de compte (ATP) de contrôle des AWS WAF fraudes pour votre site. Les étapes spécifiques que vous choisirez de suivre dépendront de vos besoins, des ressources et des demandes Web que vous recevrez.

Ces informations s'ajoutent aux informations générales sur les tests et le réglage fournies surTester et ajuster vos AWS WAF protections.

> **Note**
>
> AWS Les règles gérées sont conçues pour vous protéger contre les menaces Web les plus courantes. Lorsqu'ils sont utilisés conformément à la documentation, les groupes de règles AWS gérées ajoutent un niveau de sécurité supplémentaire à vos applications. Cependant, les groupes de règles AWS gérées ne sont pas destinés à remplacer vos responsabilités en matière de sécurité, qui sont déterminées par les AWS ressources que vous sélectionnez. Reportez-vous au modèle de responsabilité partagée pour vous assurer que vos ressources AWS sont correctement protégées.

⚠ Risque lié au trafic de production

Avant de déployer votre implémentation ATP pour le trafic de production, testez-la et ajustez-la dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite les règles en mode comptage avec votre trafic de production avant de les activer.

AWS WAF fournit des informations d'identification de test que vous pouvez utiliser pour vérifier votre configuration ATP. Dans la procédure suivante, vous allez configurer une ACL Web de test pour utiliser le groupe de règles géré par ATP, configurer une règle pour capturer l'étiquette ajoutée par le groupe de règles, puis exécuter une tentative de connexion à l'aide de ces informations d'identification de test. Vous allez vérifier que votre ACL Web a correctement géré la tentative en vérifiant les CloudWatch métriques Amazon relatives à la tentative de connexion.

Ce guide est destiné aux utilisateurs qui savent généralement comment créer et gérer des ACL, des règles et des groupes de règles AWS WAF Web. Ces sujets sont abordés dans les sections précédentes de ce guide.

Pour configurer et tester une mise en œuvre de la prévention du piratage de comptes (ATP) de contrôle des AWS WAF fraudes

Effectuez ces étapes d'abord dans un environnement de test, puis en production.

1. Ajouter le groupe de règles géré par AWS WAF Fraud Control Account Takeover Prevention (ATP) en mode décompte

   ⓘ Note

   Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d’informations, consultez Tarification d’AWS WAF.

   Ajoutez le groupe de règles AWS gérées `AWSManagedRulesATPRuleSet` à une ACL Web nouvelle ou existante et configurez-le de manière à ce qu'il ne modifie pas le comportement actuel de l'ACL Web. Pour plus de détails sur les règles et les étiquettes de ce groupe de règles, consultezAWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP).

   - Lorsque vous ajoutez le groupe de règles géré, modifiez-le et procédez comme suit :

- Dans le volet de configuration du groupe de règles, fournissez les détails de la page de connexion de votre application. Le groupe de règles ATP utilise ces informations pour surveiller les activités de connexion. Pour plus d'informations, consultez Ajouter le groupe de règles géré par ATP à votre ACL Web.
- Dans le volet Règles, ouvrez le menu déroulant Remplacer toutes les actions des règles et choisissez. Count Avec cette configuration, AWS WAF évalue les demandes par rapport à toutes les règles du groupe de règles et ne compte que les correspondances qui en résultent, tout en ajoutant des étiquettes aux demandes. Pour plus d'informations, consultez Remplacer les actions des règles dans un groupe de règles.

  Grâce à cette dérogation, vous pouvez surveiller l'impact potentiel des règles gérées par l'ATP afin de déterminer si vous souhaitez ajouter des exceptions, telles que des exceptions pour des cas d'utilisation internes.

- Positionnez le groupe de règles de manière à ce qu'il soit évalué selon vos règles existantes dans l'ACL Web, avec un paramètre de priorité numériquement supérieur à celui des règles ou groupes de règles que vous utilisez déjà. Pour plus d'informations, consultez Ordre de traitement des règles et des groupes de règles dans une ACL Web.

  Ainsi, votre gestion actuelle du trafic n'est pas perturbée. Par exemple, si vous avez des règles qui détectent le trafic malveillant tel que l'injection SQL ou les scripts intersites, elles continueront à le détecter et à le consigner. Par ailleurs, si vous avez des règles qui autorisent le trafic connu non malveillant, elles peuvent continuer à autoriser ce trafic, sans qu'il soit bloqué par le groupe de règles géré par ATP. Vous pouvez décider d'ajuster l'ordre de traitement lors de vos activités de test et de réglage.

2. Activer la journalisation et les métriques pour l'ACL Web

   Le cas échéant, configurez la journalisation, la collecte de données Amazon Security Lake, l'échantillonnage des demandes et CloudWatch les métriques Amazon pour l'ACL Web. Vous pouvez utiliser ces outils de visibilité pour surveiller l'interaction du groupe de règles géré par ATP avec votre trafic.

   - Pour plus d'informations sur la configuration et l'utilisation de la journalisation, consultezJournalisation AWS WAF du trafic ACL Web.
   - Pour plus d'informations sur Amazon Security Lake, consultez Qu'est-ce qu'Amazon Security Lake ? et Collecte de données à partir AWS des services décrits dans le guide de l'utilisateur d'Amazon Security Lake.

- Pour plus d'informations sur CloudWatch les métriques Amazon, consultezSurveillance avec Amazon CloudWatch.
- Pour plus d'informations sur l'échantillonnage des requêtes Web, consultezAffichage d'un exemple de demandes web.

3. Associer l'ACL Web à une ressource

   Si l'ACL Web n'est pas déjà associée à une ressource de test, associez-la. Pour plus d'informations, veuillez consulter Associer ou dissocier une ACL Web à une ressource AWS.

4. Surveillez le trafic et les correspondances aux règles ATP

   Assurez-vous que votre trafic normal circule et que les règles des groupes de règles gérés par ATP ajoutent des étiquettes aux requêtes Web correspondantes. Vous pouvez voir les étiquettes dans les journaux, ainsi que l'ATP et les métriques relatives aux étiquettes dans les CloudWatch statistiques Amazon. Dans les journaux, les règles que vous avez remplacées pour être prises en compte dans le groupe de règles apparaissent dans le `ruleGroupList` champ « `action` set to count » et `overriddenAction` indiquent l'action de règle configurée que vous avez remplacée.

5. Testez les capacités de vérification des informations d'identification du groupe de règles

   Effectuez une tentative de connexion en testant les informations d'identification compromises et vérifiez que le groupe de règles correspond à celles-ci comme prévu.

   a. Connectez-vous à la page de connexion de votre ressource protégée à l'aide de la paire d'identifiants de AWS WAF test suivante :

      - Utilisateur : `WAF_TEST_CREDENTIAL@wafexample.com`
      - Mot de passe : `WAF_TEST_CREDENTIAL_PASSWORD`

      Ces informations d'identification de test sont classées dans la catégorie des informations d'identification compromises, et le groupe de règles géré par ATP ajoutera l'`awswaf:managed:aws:atp:signal:credential_compromised`étiquette à la demande de connexion, que vous pouvez voir dans les journaux.

   b. Dans vos journaux ACL Web, recherchez l'`awswaf:managed:aws:atp:signal:credential_compromised`étiquette dans le `labels` champ des entrées du journal pour vos demandes Web de connexion de test. Pour

de plus amples informations sur la journalisation, veuillez consulter Journalisation AWS WAF du trafic ACL Web.

Après avoir vérifié que le groupe de règles capture les informations d'identification compromises comme prévu, vous pouvez prendre des mesures pour configurer sa mise en œuvre en fonction de vos besoins pour votre ressource protégée.

6. Pour les CloudFront distributions, testez la gestion des échecs de connexion du groupe de règles

   a. Effectuez un test pour chaque critère de réponse aux défaillances que vous avez configuré pour le groupe de règles ATP. Attendez au moins 10 minutes entre les tests.

      Pour tester un seul critère d'échec, identifiez une tentative de connexion qui échouera avec ce critère dans la réponse. Ensuite, à partir d'une seule adresse IP client, effectuez au moins 10 tentatives de connexion infructueuses en moins de 10 minutes.

      Après les 6 premiers échecs, la règle volumétrique des échecs de connexion devrait commencer à correspondre au reste de vos tentatives, à les étiqueter et à les compter. Il se peut que la règle omette le premier ou les deux premiers en raison de la latence.

   b. Dans vos journaux ACL Web, recherchez l'`awswaf:managed:aws:atp:aggregate:volumetric:ip:failed_login_response:high` dans le `labels` champ des entrées du journal pour vos demandes Web de connexion de test. Pour de plus amples informations sur la journalisation, veuillez consulter Journalisation AWS WAF du trafic ACL Web.

   Ces tests vérifient que vos critères d'échec correspondent à vos réponses en vérifiant que le nombre de connexions échouées dépasse les seuils de la règle`VolumetricIpFailedLoginResponseHigh`. Une fois les seuils atteints, si vous continuez à envoyer des demandes de connexion à partir de la même adresse IP, la règle continuera de correspondre jusqu'à ce que le taux d'échec tombe en dessous du seuil. Lorsque les seuils sont dépassés, la règle fait correspondre les connexions réussies ou échouées à partir de l'adresse IP.

7. Personnaliser le traitement des requêtes Web ATP

   Le cas échéant, ajoutez vos propres règles qui autorisent ou bloquent explicitement les demandes, afin de modifier la façon dont les règles ATP les traiteraient autrement.

Par exemple, vous pouvez utiliser les étiquettes ATP pour autoriser ou bloquer les demandes ou pour personnaliser le traitement des demandes. Vous pouvez ajouter une règle de correspondance d'étiquettes après le groupe de règles géré par ATP afin de filtrer les demandes étiquetées pour le traitement que vous souhaitez appliquer. Après le test, maintenez les règles ATP associées en mode décompte et conservez les décisions relatives au traitement des demandes dans votre règle personnalisée. Pour obtenir un exemple, consultez Exemple ATP : gestion personnalisée des informations d'identification manquantes ou compromises.

8. Supprimez vos règles de test et activez les paramètres du groupe de règles géré par ATP

   Selon votre situation, vous avez peut-être décidé de laisser certaines règles ATP en mode décompte. Pour les règles que vous souhaitez exécuter telles que configurées au sein du groupe de règles, désactivez le mode de comptage dans la configuration du groupe de règles ACL Web. Lorsque vous avez terminé le test, vous pouvez également supprimer les règles de correspondance de vos étiquettes de test.

9. Surveiller et régler

   Pour vous assurer que les requêtes Web sont traitées comme vous le souhaitez, surveillez attentivement votre trafic après avoir activé la fonctionnalité ATP que vous souhaitez utiliser. Ajustez le comportement selon vos besoins en annulant le nombre de règles sur le groupe de règles et en appliquant vos propres règles.

Une fois que vous aurez terminé de tester l'implémentation de votre groupe de règles ATP, si ce n'est déjà fait, nous vous recommandons vivement d'intégrer le AWS WAF JavaScript SDK dans la page de connexion de votre navigateur, afin d'améliorer les capacités de détection. AWS WAF fournit également des SDK mobiles pour intégrer les appareils iOS et Android. Pour plus d'informations sur les SDK d'intégration, consultezAWS WAF intégration d'applications clientes. Pour plus d'informations sur cette recommandation, consultezPourquoi utiliser les SDK d'intégration d'applications avec ATP.

AWS WAF Exemples de prévention des prises de contrôle des fraudes (ATP)

Cette section présente des exemples de configurations qui répondent aux cas d'utilisation courants pour les implémentations de prévention du rachat de comptes (ATP) dans le cadre du contrôle des AWS WAF fraudes.

Chaque exemple fournit une description du cas d'utilisation, puis montre la solution dans les listes JSON pour les règles configurées personnalisées.

> **Note**
>
> Vous pouvez récupérer des listes JSON telles que celles présentées dans ces exemples via le téléchargement ACL JSON sur la console Web ou l'éditeur JSON de règles, ou via les `getWebACL` opérations dans les API et l'interface de ligne de commande.

Rubriques

Exemple ATP : configuration simple

La liste JSON suivante montre un exemple d'ACL Web avec un groupe de règles géré par AWS WAF Fraud Control Account Takeover Prevention (ATP). Notez la configuration supplémentaire de la page de connexion, qui fournit au groupe de règles les informations dont il a besoin pour surveiller et gérer vos demandes de connexion. Ce JSON inclut les paramètres générés automatiquement par l'ACL Web, tels que l'espace de noms des étiquettes et l'URL d'intégration de l'application de l'ACL Web.

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
```

```
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
                                },
                                "PasswordField": {
                                  "Identifier": "/form/password"
                                }
                              },
                              "EnableRegexInPath": false
                            }
                          }
                        ]
                    }
                }
            }
        ],
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "ATPValidationAcl"
        },
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

Exemple ATP : gestion personnalisée des informations d'identification manquantes ou compromises

Par défaut, les vérifications d'identification effectuées par le groupe de règles `AWSManagedRulesATPRuleSet` traitent les demandes Web de la manière suivante :

- Informations d'identification manquantes — Libellé et demande de blocage.
- Informations d'identification compromises : étiquetez la demande, mais ne la bloquez pas et ne la comptez pas.

Pour plus de détails sur le groupe de règles et le comportement des règles, consultezAWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP).

Vous pouvez ajouter un traitement personnalisé pour les requêtes Web dont les informations d'identification sont manquantes ou compromises en procédant comme suit :

- Remplacer la **`MissingCredential`** règle par Count : cette action de dérogation permet à la règle de compter et d'étiqueter uniquement les demandes correspondantes.
- Ajouter une règle de correspondance des étiquettes avec gestion personnalisée : configurez cette règle pour qu'elle corresponde aux deux étiquettes ATP et pour effectuer votre gestion personnalisée. Par exemple, vous pouvez rediriger le client vers votre page d'inscription.

La règle suivante montre le groupe de règles géré par ATP dans l'exemple précédent, l'action de la `MissingCredential` règle étant remplacée pour être prise en compte. Cela oblige la règle à appliquer son étiquette aux demandes correspondantes, puis à ne compter que les demandes, au lieu de les bloquer.

```
"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": []
            }
        }
    }
],
```

Avec cette configuration, lorsque ce groupe de règles évalue une demande Web dont les informations d'identification sont manquantes ou compromises, il étiquette la demande, mais ne la bloque pas.

La règle suivante possède un paramètre de priorité supérieur numériquement à celui du groupe de règles précédent. AWS WAF évalue les règles dans l'ordre numérique, en commençant par le plus bas, de sorte que cette règle sera évaluée après l'évaluation du groupe de règles. La règle est

configurée pour correspondre à l'une ou l'autre des étiquettes d'identification et pour envoyer une réponse personnalisée aux demandes correspondantes.

```
"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"
      }
```

Exemple ATP : configuration de l'inspection des réponses

La liste JSON suivante montre un exemple d'ACL Web avec un groupe de règles géré par AWS WAF Fraud Control Account Takeover Prevention (ATP) configuré pour inspecter les réponses d'origine. Notez la configuration de l'inspection des réponses, qui spécifie les codes de réussite et d'état de réponse. Vous pouvez également configurer les paramètres de réussite et de réponse en fonction

des correspondances JSON entre en-tête, corps et corps. Ce JSON inclut les paramètres générés automatiquement par l'ACL Web, tels que l'espace de noms des étiquettes et l'URL d'intégration de l'application de l'ACL Web.

> **Note**
>
> L'inspection des réponses ATP n'est disponible que dans les ACL Web qui protègent les CloudFront distributions.

```
{
    "WebACL": {
        "LabelNamespace": "awswaf:111122223333:webacl:ATPModuleACL:",
        "Capacity": 50,
        "Description": "This is a test web ACL for ATP.",
        "Rules": [
            {
                "Priority": 1,
                "OverrideAction": {
                    "None": {}
                },
                "VisibilityConfig": {
                    "SampledRequestsEnabled": true,
                    "CloudWatchMetricsEnabled": true,
                    "MetricName": "AccountTakeOverValidationRule"
                },
                "Name": "DetectCompromisedUserCredentials",
                "Statement": {
                    "ManagedRuleGroupStatement": {
                        "VendorName": "AWS",
                        "Name": "AWSManagedRulesATPRuleSet",
                        "ManagedRuleGroupConfigs": [
                          {
                            "AWSManagedRulesATPRuleSet": {
                              "LoginPath": "/web/login",
                              "RequestInspection": {
                                "PayloadType": "JSON",
                                "UsernameField": {
                                  "Identifier": "/form/username"
                                },
                                "PasswordField": {
```

```
                                "Identifier": "/form/password"
                              }
                            },
                            "ResponseInspection": {
                              "StatusCode": {
                                "SuccessCodes": [
                                  200
                                ],
                                "FailureCodes": [
                                  401
                                ]
                              }
                            },
                            "EnableRegexInPath": false
                          }
                        }
                      ]
                    }
                }
            }
        ],
        "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "ATPValidationAcl"
        },
        "DefaultAction": {
            "Allow": {}
        },
        "ManagedByFirewallManager": false,
        "Id": "32q10987-65rs-4tuv-3210-98765wxyz432",
        "ARN": "arn:aws:wafv2:us-east-1:111122223333:regional/webacl/
ATPModuleACL/32q10987-65rs-4tuv-3210-98765wxyz432",
        "Name": "ATPModuleACL"
    },
    "ApplicationIntegrationURL": "https://9z87abce34ea.us-
east-1.sdk.awswaf.com/9z87abce34ea/1234567a1b10/",
    "LockToken": "6d0e6966-95c9-48b6-b51d-8e82e523b847"
}
```

AWS WAF Contrôle des robots

Avec Bot Control, vous pouvez facilement surveiller, bloquer ou limiter le débit des robots tels que les scrapers, les scanners, les robots d'exploration, les moniteurs d'état et les moteurs de recherche. Si vous utilisez le niveau d'inspection ciblé du groupe de règles, vous pouvez également défier les robots qui ne s'identifient pas eux-mêmes, rendant ainsi plus difficile et plus coûteuse l'action des robots malveillants sur votre site Web. Vous pouvez protéger vos applications à l'aide du groupe de règles géré par Bot Control seul ou en combinaison avec d'autres groupes de règles AWS gérées et vos propres AWS WAF règles personnalisées.

Bot Control inclut un tableau de bord de console qui indique la part de votre trafic actuel provenant de robots, sur la base d'un échantillonnage de demandes. Avec le groupe de règles géré par Bot Control ajouté à votre ACL Web, vous pouvez prendre des mesures contre le trafic de bots et recevoir des informations détaillées en temps réel sur le trafic de robots courant arrivant vers vos applications.

> **Note**
>
> Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d'informations, consultez Tarification d'AWS WAF.

Le groupe de règles géré par Bot Control fournit un niveau de protection commun de base qui ajoute des étiquettes aux robots qui s'identifient eux-mêmes, vérifie les robots généralement souhaitables et détecte les signatures de robots hautement fiables. Cela vous permet de surveiller et de contrôler les catégories courantes de trafic de bots.

Le groupe de règles Bot Control fournit également un niveau de protection ciblé qui permet de détecter les robots sophistiqués qui ne s'identifient pas eux-mêmes. Les protections ciblées utilisent des techniques de détection telles que l'interrogation du navigateur, la prise d'empreintes digitales et l'heuristique comportementale pour identifier le trafic de bots défectueux. En outre, les protections ciblées fournissent en option une analyse automatique par apprentissage automatique des statistiques de trafic du site Web afin de détecter les activités liées aux robots. Lorsque vous activez l'apprentissage automatique, AWS WAF utilise des statistiques sur le trafic du site Web, telles que les horodatages, les caractéristiques du navigateur et l'URL précédemment visitée, afin d'améliorer le modèle d'apprentissage automatique Bot Control.

Pour plus d'informations sur le groupe de règles géré par Bot Control, consultezAWS WAF Groupe de règles Bot Control.

Lors de l' AWS WAF évaluation d'une demande Web par rapport au groupe de règles géré par Bot Control, le groupe de règles ajoute des étiquettes aux demandes qu'il détecte comme liées au bot, par exemple la catégorie du bot et le nom du bot. Vous pouvez les comparer à ces libellés dans vos propres AWS WAF règles afin de personnaliser le traitement. Les étiquettes générées par le groupe de règles géré par Bot Control sont incluses dans les CloudWatch métriques Amazon et dans vos journaux ACL Web.

Vous pouvez également utiliser des AWS Firewall Manager AWS WAF politiques pour déployer le groupe de règles géré par Bot Control dans vos applications dans plusieurs comptes appartenant à votre organisation AWS Organizations.

AWS WAF Composants de Bot Control

Les principaux composants d'une implémentation de Bot Control sont les suivants :

- **`AWSManagedRulesBotControlRuleSet`**— Le groupe de règles géré par Bot Control dont les règles détectent et gèrent différentes catégories de robots. Ce groupe de règles ajoute des libellés aux requêtes Web qu'il détecte comme du trafic de bots.

  > **Note**
  >
  > Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d'informations, consultez Tarification d'AWS WAF.

  Le groupe de règles gérées par Bot Control fournit deux niveaux de protection parmi lesquels vous pouvez choisir :

  - Fréquent : détecte une variété de robots auto-identifiables, tels que les frameworks de scraping Web, les moteurs de recherche et les navigateurs automatisés. Les protections Bot Control à ce niveau identifient les robots courants à l'aide de techniques de détection de bots traditionnelles, telles que l'analyse statique des données des demandes. Les règles étiquettent le trafic provenant de ces robots et bloquent ceux qu'ils ne peuvent pas vérifier.
  - Ciblé : inclut les protections de niveau commun et ajoute une détection ciblée pour les robots sophistiqués qui ne s'identifient pas eux-mêmes. Des protections ciblées atténuent l'activité des robots en combinant la limitation du débit, le CAPTCHA et les défis liés au navigateur en arrière-plan.
    - **`TGT_`**— Les règles qui fournissent une protection ciblée portent des noms commençant par`TGT_`. Toutes les protections ciblées utilisent des techniques de détection telles que

l'interrogation du navigateur, la prise d'empreintes digitales et l'heuristique comportementale pour identifier le trafic de bots défectueux.

- **`TGT_ML_`**— Les règles de protection ciblées qui utilisent l'apprentissage automatique portent des noms commençant par`TGT_ML_`. Ces règles utilisent une analyse automatisée par apprentissage automatique des statistiques de trafic du site Web pour détecter les comportements anormaux indiquant une activité distribuée et coordonnée des bots. AWS WAF analyse les statistiques relatives au trafic de votre site Web, telles que les horodatages, les caractéristiques du navigateur et les URL précédemment visitées, afin d'améliorer le modèle d'apprentissage automatique de Bot Control. Les fonctionnalités d'apprentissage automatique sont activées par défaut, mais vous pouvez les désactiver dans la configuration de votre groupe de règles. Lorsque l'apprentissage automatique est désactivé, AWS WAF n'évalue pas ces règles.

Pour plus de détails, notamment des informations sur les règles du groupe de règles, consultezAWS WAF Groupe de règles Bot Control.

Vous incluez ce groupe de règles dans votre ACL Web à l'aide d'une déclaration de référence de groupe de règles géré et en indiquant le niveau d'inspection que vous souhaitez utiliser. Pour le niveau ciblé, vous indiquez également si vous souhaitez activer l'apprentissage automatique. Pour plus d'informations sur l'ajout de ce groupe de règles géré à votre ACL Web, consultezAjout du groupe de règles géré par AWS WAF Bot Control à votre ACL Web.

- Tableau de bord Bot Control : tableau de bord de surveillance des bots pour votre ACL Web, disponible via l'onglet Web ACL Bot Control. Utilisez ce tableau de bord pour surveiller votre trafic et comprendre dans quelle mesure celui-ci provient de différents types de robots. Cela peut être un point de départ pour personnaliser la gestion de votre bot, comme décrit dans cette rubrique. Vous pouvez également l'utiliser pour vérifier vos modifications et surveiller l'activité de différents robots et catégories de robots.
- JavaScript et SDK d'intégration d'applications mobiles : vous devez implémenter les SDK mobiles AWS WAF JavaScript et si vous utilisez le niveau de protection ciblé du groupe de règles Bot Control. Les règles ciblées utilisent les informations fournies par les SDK dans les jetons clients pour améliorer la détection contre les robots malveillants. Pour plus d'informations sur les kits SDK, consultez AWS WAF intégration d'applications clientes.
- Journalisation et statistiques : vous pouvez surveiller le trafic de votre bot et comprendre comment le groupe de règles géré par Bot Control évalue et gère votre trafic en étudiant les données collectées pour votre ACL Web par AWS WAF les journaux, Amazon Security Lake et Amazon CloudWatch. Les étiquettes que Bot Control ajoute à vos requêtes Web sont incluses dans les

données. Pour plus d'informations sur ces optionsJournalisation AWS WAF du trafic ACL Web, consultezSurveillance avec Amazon CloudWatch, et Qu'est-ce qu'Amazon Security Lake ? .

En fonction de vos besoins et du trafic que vous constatez, vous souhaiterez peut-être personnaliser votre implémentation de Bot Control. Voici quelques-unes des options les plus couramment utilisées.

- Instructions de portée réduite : vous pouvez exclure une partie du trafic des demandes Web évaluées par le groupe de règles géré par Bot Control en ajoutant une instruction de portée réduite dans la déclaration de référence du groupe de règles géré par Bot Control. Une instruction scope-down peut être n'importe quelle déclaration de règle imbriquable. Lorsqu'une demande ne correspond pas à l'instruction scope-down, elle est AWS WAF évaluée comme ne correspondant pas à l'instruction de référence du groupe de règles sans l'évaluer par rapport au groupe de règles. Pour plus d'informations sur les instructions de portée réduite, consultez. Déclarations de portée réduite

  Le prix du groupe de règles géré par Bot Control augmente en fonction du nombre de requêtes Web AWS WAF évaluées à l'aide de ce groupe. Vous pouvez contribuer à réduire ces coûts en utilisant une instruction scope-down pour limiter les demandes évaluées par le groupe de règles. Par exemple, vous pouvez autoriser le chargement de votre page d'accueil pour tout le monde, y compris les robots, puis appliquer les règles du groupe de règles aux demandes destinées aux API de votre application ou contenant un type de contenu particulier.
- Étiquettes et règles de correspondance d'étiquettes : vous pouvez personnaliser la façon dont le groupe de règles Bot Control gère une partie du trafic de robots qu'il identifie à l'aide de l'instruction de règle de correspondance des AWS WAF étiquettes. Le groupe de règles Bot Control ajoute des étiquettes à vos requêtes Web. Vous pouvez ajouter des règles de correspondance d'étiquettes après le groupe de règles Bot Control qui correspondent aux étiquettes Bot Control et appliquer le traitement dont vous avez besoin. Pour plus d'informations sur l'étiquetage et l'utilisation des instructions de correspondance des étiquettes, consultez Déclaration relative à la règle de correspondance des étiquettes etAWS WAF étiquettes sur les requêtes Web.
- Demandes et réponses personnalisées — Vous pouvez ajouter des en-têtes personnalisés aux demandes que vous autorisez et vous pouvez envoyer des réponses personnalisées pour les demandes que vous bloquez en associant l'étiquette correspondant aux fonctionnalités de demande et de réponse AWS WAF personnalisées. Pour plus d'informations sur la personnalisation des demandes et des réponses, consultezDemandes et réponses Web personnalisées dans AWS WAF.

Pourquoi utiliser les SDK d'intégration d'applications avec Bot Control

La plupart des protections ciblées du groupe de règles géré par Bot Control nécessitent les jetons de défi générés par les SDK d'intégration d'applications. Les règles qui ne nécessitent pas de jeton de défi sur la demande sont les protections de niveau commun Bot Control et les règles d'apprentissage automatique de niveau ciblé. Pour une description des niveaux de protection et des règles du groupe de règles, consultezAWS WAF Groupe de règles Bot Control.

Nous vous recommandons vivement de mettre en œuvre les SDK d'intégration d'applications, afin d'utiliser le plus efficacement possible le groupe de règles Bot Control. Le script de défi doit être exécuté avant le groupe de règles Bot Control pour que le groupe de règles puisse bénéficier des jetons acquis par le script.

- Avec les SDK d'intégration des applications, le script s'exécute automatiquement.
- Si vous ne parvenez pas à utiliser les SDK, vous pouvez configurer votre ACL Web afin qu'elle exécute l'action de CAPTCHA règle Challenge or contre toutes les demandes qui seront inspectées par le groupe de règles Bot Control. L'utilisation de l'action Challenge ou de la CAPTCHA règle peut entraîner des frais supplémentaires. Pour plus d'informations sur la tarification, consultez la page AWS WAF Pricing (Tarification).

Lorsque vous implémentez les SDK d'intégration d'applications dans vos clients ou que vous utilisez l'une des actions de règle qui exécute le script de défi, vous étendez les fonctionnalités du groupe de règles et la sécurité globale de vos applications clientes.

Les jetons fournissent des informations sur le client à chaque demande Web. Ces informations supplémentaires permettent au groupe de règles Bot Control de séparer les sessions clients légitimes des sessions client mal gérées, même lorsque les deux proviennent d'une seule adresse IP. Le groupe de règles utilise les informations contenues dans les jetons pour agréger le comportement des demandes de session client afin de permettre une détection et une atténuation précises fournies par le niveau de protection ciblé.

Pour plus d'informations sur les SDK, consultezAWS WAF intégration d'applications clientes. Pour plus d'informations sur AWS WAF les jetons, consultezAWS WAF jetons de demande Web. Pour plus d'informations sur les actions des règles, consultezCAPTCHAet Challenge dans AWS WAF.

Ajout du groupe de règles géré par AWS WAF Bot Control à votre ACL Web

Le groupe de règles géré par Bot Control `AWSManagedRulesBotControlRuleSet` nécessite une configuration supplémentaire pour identifier le niveau de protection que vous souhaitez implémenter.

Pour la description du groupe de règles et la liste des règles, voirAWS WAF Groupe de règles Bot Control.

Ce guide est destiné aux utilisateurs qui savent généralement comment créer et gérer des ACL, des règles et des groupes de règles AWS WAF Web. Ces sujets sont abordés dans les sections précédentes de ce guide. Pour obtenir des informations de base sur la façon d'ajouter un groupe de règles géré à votre ACL Web, consultezAjout d'un groupe de règles géré à une ACL Web via la console.

Suivez les meilleures pratiques

Utilisez le groupe de règles Bot Control conformément aux meilleures pratiques deMeilleures pratiques pour une atténuation intelligente des menaces.

Pour utiliser le groupe de **`AWSManagedRulesBotControlRuleSet`** règles dans votre ACL Web

1. Ajoutez le groupe de règles AWS géré `AWSManagedRulesBotControlRuleSet` à votre ACL Web. Pour la description complète du groupe de règles, voirthe section called “Groupe de règles Bot Control”.

   > **Note**
   >
   > Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d’informations, consultez Tarification d’AWS WAF.

   Lorsque vous ajoutez le groupe de règles, modifiez-le pour ouvrir la page de configuration du groupe de règles.
2. Sur la page de configuration du groupe de règles, dans le volet Niveau d'inspection, sélectionnez le niveau d'inspection que vous souhaitez utiliser.

   - Fréquent : détecte une variété de robots auto-identifiables, tels que les frameworks de scraping Web, les moteurs de recherche et les navigateurs automatisés. Les protections Bot Control à ce niveau identifient les robots courants à l'aide de techniques de détection de bots traditionnelles, telles que l'analyse statique des données des demandes. Les règles étiquettent le trafic provenant de ces robots et bloquent ceux qu'ils ne peuvent pas vérifier.
   - Ciblé : inclut les protections de niveau commun et ajoute une détection ciblée pour les robots sophistiqués qui ne s'identifient pas eux-mêmes. Des protections ciblées atténuent l'activité

des robots en combinant la limitation du débit, le CAPTCHA et les défis liés au navigateur en arrière-plan.

- **`TGT_`**— Les règles qui fournissent une protection ciblée portent des noms commençant par`TGT_`. Toutes les protections ciblées utilisent des techniques de détection telles que l'interrogation du navigateur, la prise d'empreintes digitales et l'heuristique comportementale pour identifier le trafic de bots défectueux.
- **`TGT_ML_`**— Les règles de protection ciblées qui utilisent l'apprentissage automatique portent des noms commençant par`TGT_ML_`. Ces règles utilisent une analyse automatisée par apprentissage automatique des statistiques de trafic du site Web pour détecter les comportements anormaux indiquant une activité distribuée et coordonnée des bots. AWS WAF analyse les statistiques relatives au trafic de votre site Web, telles que les horodatages, les caractéristiques du navigateur et les URL précédemment visitées, afin d'améliorer le modèle d'apprentissage automatique de Bot Control. Les fonctionnalités d'apprentissage automatique sont activées par défaut, mais vous pouvez les désactiver dans la configuration de votre groupe de règles. Lorsque l'apprentissage automatique est désactivé, AWS WAF n'évalue pas ces règles.

3. Si vous utilisez le niveau de protection ciblé et que vous ne AWS WAF souhaitez pas utiliser le machine learning (ML) pour analyser le trafic Web afin de détecter l'activité distribuée et coordonnée des bots, désactivez l'option d'apprentissage automatique. L'apprentissage automatique est requis pour les règles de contrôle des robots dont le nom commence par`TGT_ML_`. Pour plus de détails sur ces règles, consultezListe des règles de contrôle des bots.
4. Ajoutez une déclaration de portée réduite pour le groupe de règles, afin de contenir les coûts liés à son utilisation. Une instruction scope-down réduit l'ensemble des demandes inspectées par le groupe de règles. Par exemple, les cas d'utilisation, commencez par Exemple de Bot Control : utilisez Bot Control uniquement pour la page de connexion etExemple de contrôle des robots : utilisez le contrôle des robots uniquement pour le contenu dynamique.
5. Fournissez toute configuration supplémentaire dont vous avez besoin pour le groupe de règles.
6. Enregistrez les modifications apportées à l'ACL Web.

Avant de déployer votre implémentation Bot Control pour le trafic de production, testez-la et ajustez-la dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite les règles en mode comptage avec votre trafic de production avant de les activer. Consultez les sections qui suivent pour obtenir des conseils.

Faux positifs avec AWS WAF Bot Control

Nous avons soigneusement sélectionné les règles du groupe de règles géré par AWS WAF Bot Control afin de minimiser les faux positifs. Nous testons les règles par rapport au trafic mondial et surveillons leur impact sur les ACL Web de test. Cependant, il est toujours possible d'obtenir des faux positifs en raison de modifications des modèles de trafic. En outre, certains cas d'utilisation sont connus pour provoquer des faux positifs et nécessiteront une personnalisation spécifique à votre trafic Web.

Les situations dans lesquelles vous pourriez rencontrer des faux positifs sont les suivantes :

- Les applications mobiles ont généralement des agents utilisateurs autres que le navigateur, que la `SignalNonBrowserUserAgent` règle bloque par défaut. Si vous attendez du trafic provenant d'applications mobiles ou de tout autre trafic légitime impliquant des agents utilisateurs autres que les navigateurs, vous devez ajouter une exception pour l'autoriser.
- Vous pouvez vous fier à un trafic de bots spécifique pour des tâches telles que la surveillance de la disponibilité, les tests d'intégration ou les outils marketing. Si Bot Control identifie et bloque le trafic de bots que vous souhaitez autoriser, vous devez modifier le traitement en ajoutant vos propres règles. Bien qu'il ne s'agisse pas d'un scénario faussement positif pour tous les clients, si c'est pour vous, vous devrez le gérer de la même manière que pour un faux positif.
- Le groupe de règles géré par Bot Control vérifie les robots à l'aide des adresses IP de AWS WAF. Si vous utilisez Bot Control et que vous avez vérifié les bots qui acheminent via un proxy ou un équilibreur de charge, vous devrez peut-être les autoriser explicitement à l'aide d'une règle personnalisée. Pour plus d'informations sur la création d'une règle personnalisée de ce type, consultezAdresse IP transférée.
- Une règle de contrôle des bots présentant un faible taux global de faux positifs peut avoir un impact important sur des appareils ou des applications spécifiques. Par exemple, lors des tests et de la validation, nous n'avons peut-être pas observé de demandes provenant d'applications à faible volume de trafic ou de navigateurs ou d'appareils moins courants.
- Une règle de contrôle des robots dont le taux de faux positifs est historiquement bas peut avoir augmenté le nombre de faux positifs pour le trafic valide. Cela peut être dû à de nouveaux modèles de trafic ou à de nouveaux attributs de demande qui apparaissent avec un trafic valide, le faisant correspondre à la règle alors qu'il ne le faisait pas auparavant. Ces modifications peuvent être dues à des situations telles que les suivantes :
  - Détails du trafic qui sont modifiés lorsque le trafic passe par des appareils réseau, tels que les équilibreurs de charge ou les réseaux de distribution de contenu (CDN).

- Changements émergents dans les données de trafic, par exemple de nouveaux navigateurs ou de nouvelles versions de navigateurs existants.

Pour plus d'informations sur la façon de gérer les faux positifs que vous pourriez obtenir du groupe de règles géré par AWS WAF Bot Control, consultez les instructions de la section suivante,Tester et déployer AWS WAF Bot Control.

Tester et déployer AWS WAF Bot Control

Cette section fournit des conseils généraux pour configurer et tester une implémentation de AWS WAF Bot Control pour votre site. Les étapes spécifiques que vous choisirez de suivre dépendront de vos besoins, de vos ressources et des demandes Web que vous recevrez.

Ces informations s'ajoutent aux informations générales sur les tests et le réglage fournies surTester et ajuster vos AWS WAF protections.

> **Note**
>
> AWS Les règles gérées sont conçues pour vous protéger contre les menaces Web les plus courantes. Lorsqu'ils sont utilisés conformément à la documentation, les groupes de règles AWS gérées ajoutent un niveau de sécurité supplémentaire à vos applications. Cependant, les groupes de règles AWS gérées ne sont pas destinés à remplacer vos responsabilités en matière de sécurité, qui sont déterminées par les AWS ressources que vous sélectionnez. Reportez-vous au modèle de responsabilité partagée pour vous assurer que vos ressources AWS sont correctement protégées.

> **Risque lié au trafic de production**
>
> Avant de déployer votre implémentation Bot Control pour le trafic de production, testez-la et ajustez-la dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite les règles en mode comptage avec votre trafic de production avant de les activer.

Ce guide est destiné aux utilisateurs qui savent généralement comment créer et gérer des ACL, des règles et des groupes de règles AWS WAF Web. Ces sujets sont abordés dans les sections précédentes de ce guide.

Pour configurer et tester une implémentation de Bot Control

Effectuez ces étapes d'abord dans un environnement de test, puis en production.

1. Ajouter le groupe de règles géré par Bot Control

   > **Note**
   >
   > Des frais supplémentaires vous sont facturés lorsque vous utilisez ce groupe de règles géré. Pour plus d'informations, consultez Tarification d'AWS WAF.

   Ajoutez le groupe de AWS règles géré `AWSManagedRulesBotControlRuleSet` à une ACL Web nouvelle ou existante et configurez-le de manière à ce qu'il ne modifie pas le comportement actuel de l'ACL Web.

   - Lorsque vous ajoutez le groupe de règles géré, modifiez-le et procédez comme suit :
     - Dans le volet Niveau d'inspection, sélectionnez le niveau d'inspection que vous souhaitez utiliser.
       - Fréquent : détecte une variété de robots auto-identifiables, tels que les frameworks de scraping Web, les moteurs de recherche et les navigateurs automatisés. Les protections Bot Control à ce niveau identifient les robots courants à l'aide de techniques de détection de bots traditionnelles, telles que l'analyse statique des données des demandes. Les règles étiquettent le trafic provenant de ces robots et bloquent ceux qu'ils ne peuvent pas vérifier.
       - Ciblé : inclut les protections de niveau commun et ajoute une détection ciblée pour les robots sophistiqués qui ne s'identifient pas eux-mêmes. Des protections ciblées atténuent l'activité des robots en combinant la limitation du débit, les CAPTCHA et les défis liés au navigateur en arrière-plan.
         - **`TGT_`**— Les règles qui fournissent une protection ciblée portent des noms commençant par`TGT_`. Toutes les protections ciblées utilisent des techniques de détection telles que l'interrogation du navigateur, la prise d'empreintes digitales et l'heuristique comportementale pour identifier le trafic de bots défectueux.
         - **`TGT_ML_`**— Les règles de protection ciblées qui utilisent l'apprentissage automatique portent des noms commençant par`TGT_ML_`. Ces règles utilisent une analyse automatisée par apprentissage automatique des statistiques de trafic du site Web pour détecter les comportements anormaux indiquant une activité distribuée et coordonnée

des bots. AWS WAF analyse les statistiques relatives au trafic de votre site Web, telles que les horodatages, les caractéristiques du navigateur et les URL précédemment visitées, afin d'améliorer le modèle d'apprentissage automatique de Bot Control. Les fonctionnalités d'apprentissage automatique sont activées par défaut, mais vous pouvez les désactiver dans la configuration de votre groupe de règles. Lorsque l'apprentissage automatique est désactivé, AWS WAF n'évalue pas ces règles.

Pour plus d'informations sur ce choix, consultezAWS WAF Groupe de règles Bot Control.

- Dans le volet Règles, ouvrez le menu déroulant Remplacer toutes les actions des règles et choisissez. Count Avec cette configuration, AWS WAF évalue les demandes par rapport à toutes les règles du groupe de règles et ne compte que les correspondances qui en résultent, tout en ajoutant des étiquettes aux demandes. Pour plus d'informations, consultez Remplacer les actions des règles dans un groupe de règles.

  Grâce à cette dérogation, vous pouvez surveiller l'impact potentiel des règles de contrôle des bots sur votre trafic, afin de déterminer si vous souhaitez ajouter des exceptions pour des éléments tels que les cas d'utilisation internes ou les robots souhaités.

- Positionnez le groupe de règles de manière à ce qu'il soit évalué en dernier dans l'ACL Web, avec un paramètre de priorité numériquement supérieur à celui des autres règles ou groupes de règles que vous utilisez déjà. Pour plus d'informations, consultez Ordre de traitement des règles et des groupes de règles dans une ACL Web.

  Ainsi, votre gestion actuelle du trafic n'est pas perturbée. Par exemple, si vous avez des règles qui détectent le trafic malveillant tel que l'injection SQL ou les scripts intersites, elles continueront à détecter et à enregistrer ces demandes. Par ailleurs, si vous avez des règles qui autorisent le trafic connu non malveillant, elles peuvent continuer à autoriser ce trafic, sans qu'il soit bloqué par le groupe de règles géré par Bot Control. Vous pouvez décider d'ajuster l'ordre de traitement lors de vos activités de test et de réglage, mais c'est une bonne façon de commencer.

2. Activer la journalisation et les métriques pour l'ACL Web

   Le cas échéant, configurez la journalisation, la collecte de données Amazon Security Lake, l'échantillonnage des demandes et CloudWatch les métriques Amazon pour l'ACL Web. Vous pouvez utiliser ces outils de visibilité pour surveiller l'interaction du groupe de règles géré par Bot Control avec votre trafic.

   - Pour de plus amples informations sur la journalisation, veuillez consulter Journalisation AWS WAF du trafic ACL Web.

- Pour plus d'informations sur Amazon Security Lake, consultez Qu'est-ce qu'Amazon Security Lake ? et Collecte de données à partir AWS des services décrits dans le guide de l'utilisateur d'Amazon Security Lake.
- Pour plus d'informations sur CloudWatch les métriques Amazon, consultezSurveillance avec Amazon CloudWatch.
- Pour plus d'informations sur l'échantillonnage des requêtes Web, consultezAffichage d'un exemple de demandes web.

3. Associer l'ACL Web à une ressource

   Si l'ACL Web n'est pas déjà associée à une ressource, associez-la. Pour plus d'informations, veuillez consulter Associer ou dissocier une ACL Web à une ressource AWS.

4. Surveillez le trafic et les correspondances aux règles du Bot Control

   Assurez-vous que le trafic circule et que les règles du groupe de règles géré par Bot Control ajoutent des étiquettes aux requêtes Web correspondantes. Vous pouvez voir les étiquettes dans les journaux et voir les statistiques relatives aux robots et aux étiquettes dans les CloudWatch statistiques Amazon. Dans les journaux, les règles que vous avez remplacées pour être prises en compte dans le groupe de règles apparaissent dans le `ruleGroupList` champ « `action` set to count » et `overriddenAction` indiquent l'action de règle configurée que vous avez remplacée.

   > **Note**
   >
   > Le groupe de règles géré par Bot Control vérifie les robots à l'aide des adresses IP de AWS WAF. Si vous utilisez Bot Control et que vous avez vérifié les bots qui acheminent via un proxy ou un équilibreur de charge, vous devrez peut-être les autoriser explicitement à l'aide d'une règle personnalisée. Pour plus d'informations sur la création d'une règle personnalisée, consultezAdresse IP transférée. Pour plus d'informations sur la façon dont vous pouvez utiliser la règle pour personnaliser le traitement des requêtes Web par Bot Control, reportez-vous à l'étape suivante.

   Examinez attentivement le traitement des requêtes Web pour détecter tout faux positif que vous pourriez avoir besoin d'atténuer grâce à un traitement personnalisé. Pour des exemples de faux positifs, voirFaux positifs avec AWS WAF Bot Control.

5. Personnaliser le traitement des requêtes Web par Bot Control

   Le cas échéant, ajoutez vos propres règles qui autorisent ou bloquent explicitement les demandes, afin de modifier la façon dont les règles de contrôle des bots les traiteraient autrement.

   La manière de procéder dépend de votre cas d'utilisation, mais les solutions les plus courantes sont les suivantes :

   - Autorisez explicitement les demandes avec une règle que vous ajoutez avant le groupe de règles géré par Bot Control. Ainsi, les demandes autorisées n'atteignent jamais le groupe de règles pour être évaluées. Cela peut aider à réduire les coûts liés à l'utilisation du groupe de règles géré par Bot Control.
   - Excluez les demandes de l'évaluation de Bot Control en ajoutant une instruction scope-down dans l'instruction du groupe de règles géré par Bot Control. Cela fonctionne de la même manière que l'option précédente. Cela peut aider à réduire les coûts liés à l'utilisation du groupe de règles géré par Bot Control, car les demandes qui ne correspondent pas à l'instruction scope-down ne sont jamais évaluées par le groupe de règles. Pour plus d'informations sur les instructions de portée réduite, voir. Déclarations de portée réduite

     Pour obtenir des exemples relatifs à , consultez les rubriques suivantes :

     - Exclure la plage d'adresses IP de la gestion des robots
     - Autoriser le trafic provenant d'un bot que vous contrôlez
   - Utilisez les étiquettes Bot Control dans le traitement des demandes pour autoriser ou bloquer les demandes. Ajoutez une règle de correspondance des libellés après le groupe de règles géré par Bot Control pour filtrer les demandes étiquetées que vous souhaitez autoriser de celles que vous souhaitez bloquer.

     Après le test, maintenez les règles de contrôle des robots associées en mode décompte et conservez les décisions relatives au traitement des demandes dans votre règle personnalisée. Pour plus d'informations sur les déclarations de correspondance des étiquettes, voirDéclaration relative à la règle de correspondance des étiquettes.

     Pour des exemples de ce type de personnalisation, consultez les pages suivantes :

     - Création d'une exception pour un agent utilisateur bloqué
     - Autoriser un bot bloqué spécifique
     - Bloquer les robots vérifiés

Pour accéder à des exemples supplémentaires, consultez AWS WAF Exemples de Bot Control.

6. Si nécessaire, activez les paramètres du groupe de règles géré par Bot Control

   En fonction de votre situation, vous avez peut-être décidé de laisser certaines règles de contrôle des bots en mode décompte ou de les remplacer par une autre action. Pour les règles que vous souhaitez exécuter telles qu'elles sont configurées dans le groupe de règles, activez la configuration des règles standard. Pour ce faire, modifiez l'instruction du groupe de règles dans votre ACL Web et apportez vos modifications dans le volet Règles.

AWS WAF Exemples de Bot Control

Cette section présente des exemples de configurations qui répondent à divers cas d'utilisation courants pour les implémentations de AWS WAF Bot Control.

Chaque exemple fournit une description du cas d'utilisation, puis montre la solution dans les listes JSON pour les règles configurées personnalisées.

> **Note**
>
> Les listes JSON présentées dans ces exemples ont été créées dans la console en configurant la règle, puis en la modifiant à l'aide de l'éditeur Rule JSON.

Rubriques

- Exemple de contrôle des bots : niveau d'inspection ciblé
- Exemple de contrôle des robots : utilisez deux instructions pour limiter l'utilisation du niveau d'inspection ciblé

Exemple de contrôle des robots : configuration simple

La liste JSON suivante montre un exemple d'ACL Web avec un groupe de règles géré par AWS WAF Bot Control. Notez la configuration de visibilité, qui entraîne le stockage AWS WAF d'échantillons de demandes et de mesures à des fins de surveillance.

```
{
  "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
}
```

Exemple de contrôle des bots : autorisez explicitement les robots vérifiés

AWS WAF Le contrôle des bots ne bloque pas les robots connus AWS pour être des robots courants et vérifiables. Lorsque Bot Control identifie une demande Web comme provenant d'un bot vérifié, il ajoute une étiquette qui nomme le bot et une étiquette qui indique qu'il s'agit d'un bot vérifié. Bot Control n'ajoute aucune autre étiquette, telle que des étiquettes de signaux, afin d'empêcher le blocage des robots connus pour leur bon fonctionnement.

Il se peut que d'autres AWS WAF règles bloquent les robots vérifiés. Si vous souhaitez vous assurer que les robots vérifiés sont autorisés, ajoutez une règle personnalisée pour les autoriser en fonction des étiquettes Bot Control. Votre nouvelle règle doit être exécutée après le groupe de règles géré par Bot Control, afin que les étiquettes puissent être comparées.

La règle suivante autorise explicitement les robots vérifiés.

```
{
    "Name": "match_rule",
    "Statement": {
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Allow": {}
    }
}
```

Exemple de contrôle des bots : bloquez les robots vérifiés

Pour bloquer les robots vérifiés, vous devez ajouter une règle de blocage qui s'exécute après le groupe de règles géré par AWS WAF Bot Control. Pour ce faire, identifiez les noms des robots que vous souhaitez bloquer et utilisez une instruction label match pour les identifier et les bloquer. Si vous souhaitez simplement bloquer tous les robots vérifiés, vous pouvez omettre la correspondance avec l'`bot:name:`étiquette.

La règle suivante bloque uniquement le bot `bingbot` vérifié. Cette règle doit être exécutée après le groupe de règles géré par Bot Control.

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:name:bingbot"
            }
          },
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:bot:verified"
            }
          }
        ]
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
  }
```

La règle suivante bloque tous les robots vérifiés.

```
{
    "Name": "match_rule",
    "Statement": {
```

```
      "LabelMatchStatement": {
        "Scope": "LABEL",
        "Key": "awswaf:managed:aws:bot-control:bot:verified"
      }
    },
    "RuleLabels": [],
    "Action": {
      "Block": {}
    }
}
```

Exemple de contrôle des bots : autoriser un bot bloqué spécifique

Il est possible qu'un bot soit bloqué par plusieurs règles de contrôle des robots. Exécutez la procédure suivante pour chaque règle de blocage.

Si une AWS WAF règle de contrôle des bots bloque un bot que vous ne souhaitez pas bloquer, procédez comme suit :

1. Identifiez la règle de contrôle du bot qui bloque le bot en consultant les journaux. La règle de blocage sera spécifiée dans les journaux dans les champs dont le nom commence par`terminatingRule`. Pour plus d'informations sur les journaux ACL Web, consultezJournalisation AWS WAF du trafic ACL Web. Notez l'étiquette que la règle ajoute aux demandes.
2. Dans votre ACL Web, remplacez l'action de la règle de blocage pour compter. Pour ce faire, dans la console, modifiez la règle du groupe de règles dans l'ACL Web et choisissez une action de remplacement Count pour la règle. Cela garantit que le bot n'est pas bloqué par la règle, mais que la règle appliquera toujours son étiquette aux demandes correspondantes.
3. Ajoutez une règle de correspondance d'étiquettes à votre ACL Web, après le groupe de règles géré par Bot Control. Configurez la règle pour qu'elle corresponde à l'étiquette de la règle remplacée et pour bloquer toutes les demandes correspondantes, à l'exception du bot que vous ne souhaitez pas bloquer.

   Votre ACL Web est désormais configurée de telle sorte que le bot que vous souhaitez autoriser ne soit plus bloqué par la règle de blocage que vous avez identifiée dans les journaux.

Vérifiez à nouveau le trafic et vos journaux pour vous assurer que le bot est autorisé à entrer. Si ce n'est pas le cas, réexécutez la procédure ci-dessus.

Supposons, par exemple, que vous souhaitiez bloquer tous les robots de surveillance à l'exception de`pingdom`. Dans ce cas, vous remplacez la `CategoryMonitoring` règle pour compter, puis vous rédigez une règle pour bloquer tous les robots de surveillance, à l'exception de ceux portant le nom du bot. `pingdom`

La règle suivante utilise le groupe de règles géré par Bot Control mais remplace l'action de la règle pour qu'elle soit prise `CategoryMonitoring` en compte. La règle de surveillance des catégories applique ses étiquettes comme d'habitude aux demandes correspondantes, mais les compte uniquement au lieu d'effectuer son action habituelle de blocage.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "CategoryMonitoring"
        }
      ],
      "ExcludedRules": []
    }
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "AWS-AWSBotControl-Example"
  }
}
```

La règle suivante correspond à l'étiquette de surveillance des catégories que la `CategoryMonitoring` règle précédente ajoute aux requêtes Web correspondantes. Parmi les demandes de surveillance des catégories, cette règle bloque toutes sauf celles dont le nom du bot est étiquetépingdom.

La règle suivante doit être exécutée après le groupe de règles géré par Bot Control précédent dans l'ordre de traitement de l'ACL Web.

```
{
      "Name": "match_rule",
      "Priority": 10,
      "Statement": {
        "AndStatement": {
          "Statements": [
            {
              "LabelMatchStatement": {
                "Scope": "LABEL",
                "Key": "awswaf:managed:aws:bot-control:bot:category:monitoring"
              }
            },
            {
              "NotStatement": {
                "Statement": {
                  "LabelMatchStatement": {
                    "Scope": "LABEL",
                    "Key": "awswaf:managed:aws:bot-control:bot:name:pingdom"
                  }
                }
              }
            }
          ]
        }
      },
      "Action": {
        "Block": {}
      },
      "VisibilityConfig": {
        "SampledRequestsEnabled": true,
        "CloudWatchMetricsEnabled": true,
        "MetricName": "match_rule"
      }
}
```

Exemple de contrôle des bots : création d'une exception pour un agent utilisateur bloqué

Si le trafic provenant de certains agents utilisateurs autres que le navigateur est bloqué par erreur, vous pouvez créer une exception en définissant la règle `SignalNonBrowserUserAgent` de contrôle des AWS WAF bots incriminée sur Nombre, puis en combinant l'étiquetage de la règle avec vos critères d'exception.

> **Note**
>
> Les applications mobiles ont généralement des agents utilisateurs autres que le navigateur, que la `SignalNonBrowserUserAgent` règle bloque par défaut.

La règle suivante utilise le groupe de règles géré par Bot Control mais remplace l'action de règle pour `SignalNonBrowserUserAgent` to Count. La règle du signal applique ses étiquettes comme d'habitude aux demandes correspondantes, mais les compte uniquement au lieu d'effectuer son action habituelle de blocage.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
   "RuleActionOverrides": [
        {
          "ActionToUse": {
            "Count": {}
          },
          "Name": "SignalNonBrowserUserAgent"
        }
      ],
      "ExcludedRules": []
```

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

La règle suivante correspond à l'étiquette de signal que la `SignalNonBrowserUserAgent` règle Bot Control ajoute à ses requêtes Web correspondantes. Parmi les demandes de signal, cette règle bloque toutes sauf celles qui ont l'agent utilisateur que nous voulons autoriser.

La règle suivante doit être exécutée après le groupe de règles géré par Bot Control précédent dans l'ordre de traitement de l'ACL Web.

```
{
    "Name": "match_rule",
    "Statement": {
      "AndStatement": {
        "Statements": [
          {
            "LabelMatchStatement": {
              "Scope": "LABEL",
              "Key": "awswaf:managed:aws:bot-control:signal:non_browser_user_agent"
            }
          },
          {
            "NotStatement": {
              "Statement": {
                "ByteMatchStatement": {
                  "FieldToMatch": {
                    "SingleHeader": {
                      "Name": "user-agent"
                    }
                  },
                  "PositionalConstraint": "EXACTLY",
                  "SearchString": "PostmanRuntime/7.29.2",
                  "TextTransformations": [
                    {
                      "Priority": 0,
                      "Type": "NONE"
                    }
```

```
                ]
              }
            }
          }
        }
      ]
    }
  },
  "RuleLabels": [],
  "Action": {
    "Block": {}
  },
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
    "CloudWatchMetricsEnabled": true,
    "MetricName": "match_rule"
  }
}
```

Exemple de Bot Control : utilisez Bot Control uniquement pour la page de connexion

L'exemple suivant utilise une instruction scope-down pour appliquer le contrôle des AWS WAF robots uniquement au trafic arrivant sur la page de connexion d'un site Web, qui est identifiée par le chemin de l'URI. `login` Le chemin de l'URI vers votre page de connexion peut être différent de celui indiqué dans l'exemple, en fonction de votre application et de votre environnement.

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

Exemple de contrôle des robots : utilisez le contrôle des robots uniquement pour le contenu dynamique

Cet exemple utilise une instruction scope-down pour appliquer le contrôle des AWS WAF robots uniquement au contenu dynamique.

L'instruction scope-down exclut le contenu statique en annulant les résultats de correspondance pour un ensemble de modèles regex :

- L'ensemble de modèles regex est configuré pour correspondre aux extensions de contenu statique. Par exemple, la spécification du jeu de modèles regex peut être`(?i)\.(jpe?g|gif|png|svg|ico|css|js|woff2?)$`. Pour plus d'informations sur les ensembles de modèles et les instructions regex, consultezInstruction de correspondance d'ensemble de modèles d'expression régulière de règle.
- Dans l'instruction scope-down, nous excluons le contenu statique correspondant en imbriquant l'instruction regex pattern set dans une instruction. `NOT` Pour plus d'informations sur `NOT` cette déclaration, voirNOTdéclaration de règle.

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

Exemple de contrôle des robots : exclure une plage d'adresses IP de la gestion des robots

Si vous souhaitez exclure un sous-ensemble du trafic Web de la gestion de AWS WAF Bot Control et que vous pouvez identifier ce sous-ensemble à l'aide d'une instruction de règle, excluez-le en ajoutant une instruction de portée vers le bas à votre déclaration de groupe de règles géré par Bot Control.

La règle suivante exécute la gestion normale du bot Bot Control sur l'ensemble du trafic Web, à l'exception des requêtes Web provenant d'une plage d'adresses IP spécifique.

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

```
}
```

Exemple de contrôle des robots : autoriser le trafic provenant d'un bot que vous contrôlez

Vous pouvez configurer certains robots de surveillance du site et certains robots personnalisés pour envoyer des en-têtes personnalisés. Si vous souhaitez autoriser le trafic provenant de ces types de robots, vous pouvez les configurer pour ajouter un secret partagé dans un en-tête. Vous pouvez ensuite exclure les messages comportant un en-tête en ajoutant une instruction scope-down à l'instruction du groupe de règles géré par AWS WAF Bot Control.

L'exemple de règle suivant exclut le trafic avec un en-tête secret de l'inspection Bot Control.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "COMMON"
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "AWS-AWSBotControl-Example"
    },
    "ScopeDownStatement": {
      "NotStatement": {
        "Statement": {
          "ByteMatchStatement": {
            "SearchString": "YSBzZWNyZXQ=",
            "FieldToMatch": {
              "SingleHeader": {
                "Name": "x-bypass-secret"
              }
```

```
            },
            "TextTransformations": [
              {
                "Priority": 0,
                "Type": "NONE"
              }
            ],
            "PositionalConstraint": "EXACTLY"
          }
        }
      }
    }
  }
}
```

Exemple de contrôle des bots : niveau d'inspection ciblé

Pour un niveau de protection amélioré, vous pouvez activer le niveau d'inspection ciblé dans votre groupe de règles géré par AWS WAF Bot Control.

Dans l'exemple suivant, les fonctionnalités d'apprentissage automatique sont activées. Vous pouvez désactiver ce comportement en réglant `EnableMachineLearning` sur`false`.

```
{
  "Name": "AWS-AWSBotControl-Example",
  "Priority": 5,
  "Statement": {
    "ManagedRuleGroupStatement": {
      "VendorName": "AWS",
      "Name": "AWSManagedRulesBotControlRuleSet",
      "ManagedRuleGroupConfigs": [
        {
          "AWSManagedRulesBotControlRuleSet": {
            "InspectionLevel": "TARGETED",
            "EnableMachineLearning": true
          }
        }
      ],
      "RuleActionOverrides": [],
      "ExcludedRules": []
    },
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
```

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

Exemple de contrôle des robots : utilisez deux instructions pour limiter l'utilisation du niveau d'inspection ciblé

Pour optimiser les coûts, vous pouvez utiliser deux instructions de groupes de règles gérés par AWS WAF Bot Control dans votre ACL Web, avec des niveaux d'inspection et un périmètre distincts. Par exemple, vous pouvez étendre l'énoncé du niveau d'inspection ciblé uniquement aux points de terminaison d'application les plus sensibles.

Les deux instructions de l'exemple suivant ont une portée mutuellement exclusive. Sans cette configuration, une demande pourrait donner lieu à deux évaluations facturées.

> **Note**
>
> Le référencement d'instructions multiples `AWSManagedRulesBotControlRuleSet` n'est pas pris en charge dans l'éditeur visuel de la console. Utilisez plutôt l'éditeur JSON.

```
{
  "Name": "Bot-WebACL",
  "Id": "...",
  "ARN": "...",
  "DefaultAction": {
    "Allow": {}
  },
  "Description": "Bot-WebACL",
  "Rules": [
      {
        ...
      },
      {
       "Name": "AWS-AWSBotControl-Common",
       "Priority": 5,
       "Statement": {
          "ManagedRuleGroupStatement": {
             "VendorName": "AWS",
             "Name": "AWSManagedRulesBotControlRuleSet",
```

```
            "ManagedRuleGroupConfigs": [
              {
                "AWSManagedRulesBotControlRuleSet": {
                  "InspectionLevel": "COMMON"
                }
              }
            ],
            "RuleActionOverrides": [],
            "ExcludedRules": []
         },
         "VisibilityConfig": {
            "SampledRequestsEnabled": true,
            "CloudWatchMetricsEnabled": true,
            "MetricName": "AWS-AWSBotControl-Common"
          },
          "ScopeDownStatement": {
             "NotStatement": {
               "Statement": {
                 "ByteMatchStatement": {
                   "FieldToMatch": {
                     "UriPath": {}
                   },
                   "PositionalConstraint": "STARTS_WITH",
                   "SearchString": "/sensitive-endpoint",
                   "TextTransformations": [
                     {
                       "Type": "NONE",
                       "Priority": 0
                     }
                   ]
                 }
               }
             }
          }
      }
    },
    {
     "Name": "AWS-AWSBotControl-Targeted",
     "Priority": 6,
     "Statement": {
        "ManagedRuleGroupStatement": {
           "VendorName": "AWS",
           "Name": "AWSManagedRulesBotControlRuleSet",
           "ManagedRuleGroupConfigs": [
```

```
                {
                  "AWSManagedRulesBotControlRuleSet": {
                    "InspectionLevel": "TARGETED",
                    "EnableMachineLearning": true
                  }
                }
              ],
              "RuleActionOverrides": [],
              "ExcludedRules": []
           },
           "VisibilityConfig": {
              "SampledRequestsEnabled": true,
              "CloudWatchMetricsEnabled": true,
              "MetricName": "AWS-AWSBotControl-Targeted"
            },
            "ScopeDownStatement": {
               "Statement": {
                 "ByteMatchStatement": {
                   "FieldToMatch": {
                     "UriPath": {}
                   },
                   "PositionalConstraint": "STARTS_WITH",
                   "SearchString": "/sensitive-endpoint",
                   "TextTransformations": [
                     {
                       "Type": "NONE",
                       "Priority": 0
                     }
                   ]
                 }
               }
             }
         }
       }
    ],
    "VisibilityConfig": {
      ...
    },
    "Capacity": 1496,
    "ManagedByFirewallManager": false
}
```

AWS WAF intégration d'applications clientes

Utilisez les API d'intégration des applications AWS WAF clientes pour associer les protections côté client à vos protections ACL Web AWS côté serveur, afin de vérifier que les applications clientes qui envoient des requêtes Web à vos ressources protégées sont les clients visés et que vos utilisateurs finaux sont des êtres humains.

Utilisez les intégrations du client pour gérer les problèmes liés aux navigateurs silencieux et les puzzles CAPTCHA, obtenir des jetons prouvant que le navigateur et l'utilisateur final ont répondu avec succès, et pour inclure ces jetons dans les demandes adressées à vos terminaux protégés. Pour des informations générales sur AWS WAF les jetons, consultezAWS WAF jetons de demande Web.

Combinez vos intégrations clients avec des protections ACL Web qui nécessitent des jetons valides pour accéder à vos ressources. Vous pouvez utiliser des groupes de règles qui vérifient et surveillent les jetons de défi, comme ceux répertoriés dans la section suivanteIntégration intelligente des menaces et règles AWS gérées, à, et vous pouvez utiliser les actions de Challenge règle CAPTCHA et pour vérifier, comme décrit dansCAPTCHAet Challenge dans AWS WAF.

AWS WAF propose deux niveaux d'intégration pour les JavaScript applications et un pour les applications mobiles :

- Intégration intelligente des menaces : vérifiez l'application cliente et assurez l'acquisition et la gestion des AWS jetons. Cette fonctionnalité est similaire à celle fournie par l'action de AWS WAF Challenge règle. Cette fonctionnalité intègre complètement votre application cliente au groupe de règles `AWSManagedRulesACFPRuleSet` géré, au groupe de règles `AWSManagedRulesATPRuleSet` géré et au niveau de protection ciblé du groupe de règles `AWSManagedRulesBotControlRuleSet` géré.

  Les API d'intégration intelligente des menaces utilisent le défi du navigateur AWS WAF silencieux pour garantir que les tentatives de connexion et les autres appels à votre ressource protégée ne sont autorisés qu'une fois que le client a obtenu un jeton valide. Les API gèrent l'autorisation par jeton pour les sessions de votre application client et collectent des informations sur le client afin de déterminer s'il est géré par un robot ou par un être humain.

  > **Note**
  >
  > Ceci est disponible pour JavaScript et pour les applications mobiles Android et iOS.

- Intégration des CAPTCHA — Vérifiez les utilisateurs finaux avec un casse-tête CAPTCHA personnalisé que vous gérez dans votre application. Cette fonctionnalité est similaire à celle fournie par l'action des AWS WAF CAPTCHA règles, mais avec un contrôle accru sur le placement et le comportement du puzzle.

  Cette intégration tire parti de l'intégration JavaScript intelligente des menaces pour lancer des défis silencieux et fournir des AWS WAF jetons à la page du client.

  > **Note**
  >
  > Ceci est disponible pour les JavaScript applications.

Rubriques

- Intégration intelligente des menaces et règles AWS gérées
- Accès aux API d'intégration des applications AWS WAF clientes
- AWS WAF JavaScript intégrations
- AWS WAF intégration d'applications mobiles

Intégration intelligente des menaces et règles AWS gérées

Les API d'intégration intelligente des menaces fonctionnent avec les ACL Web qui utilisent les groupes de règles de menaces intelligents pour activer toutes les fonctionnalités de ces groupes de règles gérés avancés.

- AWS WAF Groupe `AWSManagedRulesACFPRuleSet` de règles géré par Fraud Control pour la création de comptes et la prévention des fraudes (ACFP).

  La fraude liée à la création de compte est une activité illégale en ligne dans le cadre de laquelle un attaquant crée des comptes non valides dans votre application dans le but, par exemple, de recevoir des bonus d'inscription ou de se faire passer pour quelqu'un. Le groupe de règles géré par l'ACFP fournit des règles pour bloquer, étiqueter et gérer les demandes susceptibles de faire partie de tentatives de création de compte frauduleuses. Les API permettent une vérification précise du navigateur client et des informations d'interactivité humaine que les règles ACFP utilisent pour séparer le trafic client valide du trafic malveillant.

Pour plus d'informations, consultez AWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes et AWS WAF Contrôle des fraudes : création de comptes, prévention des fraudes (ACFP).

- AWS WAF Groupe de règles géré par Fraud Control pour la prévention des prises de contrôle des comptes (ATP)`AWSManagedRulesATPRuleSet`.

  Le piratage de compte est une activité illégale en ligne par laquelle un attaquant obtient un accès non autorisé au compte d'une personne. Le groupe de règles géré par ATP fournit des règles pour bloquer, étiqueter et gérer les demandes susceptibles de faire partie de tentatives malveillantes de prise de contrôle de compte. Les API permettent une vérification précise des clients et une agrégation des comportements que les règles ATP utilisent pour séparer le trafic client valide du trafic malveillant.

  Pour plus d'informations, consultez AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP) et AWS WAF Contrôle des fraudes et prévention des prises de contrôle des comptes (ATP).

- Niveau de protection ciblé du groupe de règles géré par AWS WAF Bot Control`AWSManagedRulesBotControlRuleSet`.

  Les robots peuvent être des robots utiles et auto-identifiables, comme la plupart des moteurs de recherche et des robots d'exploration, ou des robots malveillants qui agissent contre votre site Web et ne s'identifient pas eux-mêmes. Le groupe de règles géré par Bot Control fournit des règles pour surveiller, étiqueter et gérer l'activité des robots dans votre trafic Web. Lorsque vous utilisez le niveau de protection ciblé de ce groupe de règles, les règles ciblées utilisent les informations de session client fournies par les API pour mieux détecter les robots malveillants.

  Pour plus d'informations, consultez AWS WAF Groupe de règles Bot Control et AWS WAF Contrôle des robots.

Pour ajouter l'un de ces groupes de règles gérés à votre ACL Web, consultez les procédures Ajouter le groupe de règles géré par l'ACFP à votre ACL WebAjouter le groupe de règles géré par ATP à votre ACL Web, etAjout du groupe de règles géré par AWS WAF Bot Control à votre ACL Web.

> **Note**
>
> Les groupes de règles gérés ne bloquent actuellement pas les demandes pour lesquelles il manque des jetons. Afin de bloquer les demandes pour lesquelles il manque des jetons,

une fois que vous avez implémenté les API d'intégration de vos applications, suivez les instructions surBlocage des demandes dont le AWS WAF jeton n'est pas valide.

Accès aux API d'intégration des applications AWS WAF clientes

Les API JavaScript d'intégration sont généralement disponibles et vous pouvez les utiliser pour vos navigateurs et autres appareils qui les exécutent JavaScript.

AWS WAF propose des SDK d'intégration intelligente des menaces personnalisés pour les applications mobiles Android et iOS.

- Pour les applications mobiles Android, les AWS WAF SDK fonctionnent pour la version 23 de l'API Android (Android version 6) et les versions ultérieures. Pour plus d'informations sur les versions d'Android, consultez les notes de mise à jour de SDK Platform.
- Pour les applications mobiles iOS, AWS WAF les SDK fonctionnent pour iOS version 13 et versions ultérieures. Pour plus d'informations sur les versions d'iOS, consultez les notes de mise à jour pour iOS et iPadOS.

Pour accéder aux API d'intégration via la console

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Choisissez Intégration des applications dans le volet de navigation, puis sélectionnez l'onglet qui vous intéresse.

   - L'intégration intelligente des menaces est disponible pour JavaScript les applications mobiles.

     L'onglet contient les éléments suivants :

     - Liste des ACL Web activées pour l'intégration intelligente des applications de lutte contre les menaces. La liste inclut chaque ACL Web qui utilise le groupe de règles `AWSManagedRulesACFPRuleSet` `AWSManagedRulesATPRuleSet` géré, le groupe de règles géré ou le niveau de protection ciblé du groupe de règles `AWSManagedRulesBotControlRuleSet` géré. Lorsque vous implémentez les API de menaces intelligentes, vous utilisez l'URL d'intégration de l'ACL Web à laquelle vous souhaitez effectuer l'intégration.

    - Les API auxquelles vous avez accès. Les JavaScript API sont toujours disponibles. Pour accéder aux SDK mobiles, contactez l'assistance via Contact AWS.
- L'intégration CAPTCHA est disponible pour les JavaScript applications.

  L'onglet contient les éléments suivants :

  - URL d'intégration à utiliser dans votre intégration.
  - Les clés d'API que vous avez créées pour les domaines de vos applications clientes. Votre utilisation de l'API CAPTCHA nécessite une clé d'API cryptée qui donne aux clients le droit d'accéder au AWS WAF CAPTCHA depuis leurs domaines. Pour chaque client auquel vous effectuez l'intégration, utilisez une clé d'API contenant le domaine du client. Pour plus d'informations sur ces exigences et sur la gestion de ces clés, consultezGestion des clés d'API pour l'API JS CAPTCHA.

AWS WAF JavaScript intégrations

Vous pouvez utiliser les API JavaScript d'intégration pour implémenter des intégrations AWS WAF d'applications dans vos navigateurs et les autres appareils qui s'exécutent JavaScript.

Les puzzles CAPTCHA et les défis silencieux ne peuvent être exécutés que lorsque les navigateurs accèdent à des points de terminaison HTTPS. Les clients du navigateur doivent fonctionner dans des contextes sécurisés pour acquérir des jetons.

- Les API de menaces intelligentes vous permettent de gérer l'autorisation des jetons par le biais d'un défi de navigateur silencieux côté client et d'inclure les jetons dans les demandes que vous envoyez à vos ressources protégées.
- L'API d'intégration CAPTCHA complète les API de menaces intelligentes et vous permet de personnaliser l'emplacement et les caractéristiques du puzzle CAPTCHA dans vos applications clientes. Cette API utilise les API de menaces intelligentes pour acquérir des AWS WAF jetons à utiliser sur la page une fois que l'utilisateur final a réussi à résoudre le casse-tête CAPTCHA.

En utilisant ces intégrations, vous vous assurez que les appels de procédure à distance effectués par votre client contiennent un jeton valide. Lorsque ces API d'intégration sont en place sur les pages de votre application, vous pouvez implémenter des règles d'atténuation dans votre ACL Web, telles que le blocage des demandes qui ne contiennent pas de jeton valide. Vous pouvez également implémenter des règles qui imposent l'utilisation des jetons que vos applications clientes obtiennent, en utilisant les CAPTCHA actions Challenge ou de vos règles.

La liste suivante présente les composants de base d'une implémentation typique des API de menaces intelligentes dans une page d'application Web.

```
<head>
<script type="text/javascript" src="Web ACL integration URL/challenge.js" defer></
script>
</head>
<script>
const login_response = await AwsWafIntegration.fetch(login_url, {
    method: 'POST',
    headers: {
      'Content-Type': 'application/json'
    },
    body: login_body
  });
</script>
```

L'API d'intégration CAPTCHA vous permet de personnaliser l'expérience de puzzle CAPTCHA de vos utilisateurs finaux. L'intégration CAPTCHA tire parti de l'intégration JavaScript intelligente des menaces, pour la vérification du navigateur et la gestion des jetons, et ajoute une fonction pour configurer et afficher le casse-tête CAPTCHA.

La liste suivante présente les composants de base d'une implémentation typique de l' JavaScript API CAPTCHA dans une page d'application Web.

```
<head>
    <script type="text/javascript" src="<Integration URL>/jsapi.js" defer></script>
</head>

<script type="text/javascript">
    function showMyCaptcha() {
        var container = document.querySelector("#my-captcha-container");

        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            ...other configuration parameters as needed...
        });
    }

    function captchaExampleSuccessFunction(wafToken) {
```

```
        // Use WAF token to access protected resources
        AwsWafIntegration.fetch("...WAF-protected URL...", {
            method: "POST",
            ...
        });
    }

    function captchaExampleErrorFunction(error) {
        /* Do something with the error */
    }
</script>

<div id="my-captcha-container">
    <!-- The contents of this container will be replaced by the captcha widget -->
</div>
```

Rubriques

- Fournir des domaines à utiliser dans les jetons
- Utilisation de l' JavaScript API avec des politiques de sécurité du contenu
- Utilisation de l' JavaScript API de gestion intelligente des menaces
- Utilisation de l'API CAPTCHA JavaScript

Fournir des domaines à utiliser dans les jetons

Par défaut, lors de AWS WAF la création d'un jeton, il utilise le domaine hôte de la ressource associée à l'ACL Web. Vous pouvez fournir des domaines supplémentaires pour les jetons AWS WAF créés pour les JavaScript API. Pour ce faire, configurez la variable `window.awsWafCookieDomainList` globale avec un ou plusieurs domaines de jetons.

Lors AWS WAF de la création d'un jeton, il utilise le domaine le plus approprié et le plus court parmi la combinaison des domaines `window.awsWafCookieDomainList` et du domaine hôte de la ressource associée à l'ACL Web.

Exemples de paramètres :

```
window.awsWafCookieDomainList = ['.aws.amazon.com']
```

```
window.awsWafCookieDomainList = ['.aws.amazon.com', 'abc.aws.amazon.com']
```

Vous ne pouvez pas utiliser de suffixes publics dans cette liste. Par exemple, vous ne pouvez pas utiliser `gov.au` ou `co.uk` comme domaines symboliques dans la liste.

Les domaines que vous spécifiez dans cette liste doivent être compatibles avec vos autres domaines et configurations de domaines :

- Les domaines doivent être ceux qui AWS WAF seront acceptés, en fonction du domaine hôte protégé et de la liste de domaines de jetons configurée pour l'ACL Web. Pour plus d'informations, consultez AWS WAF configuration de la liste de domaines du jeton ACL Web.
- Si vous utilisez l'API JavaScript CAPTCHA, au moins un domaine de votre clé d'API CAPTCHA doit correspondre exactement à l'un des domaines de jetons `window.awsWafCookieDomainList` ou il doit être le domaine apex de l'un de ces domaines de jetons.

  Par exemple, pour le domaine de jeton`mySubdomain.myApex.com`, la clé `mySubdomain.myApex.com` d'API correspond exactement et la clé d'API `myApex.com` est le domaine apex. L'une ou l'autre des clés correspond au domaine du jeton.

  Pour plus d'informations sur les clés d'API, consultezGestion des clés d'API pour l'API JS CAPTCHA.

Si vous utilisez le groupe de règles `AWSManagedRulesACFPRuleSet` géré, vous pouvez configurer un domaine qui correspond à celui indiqué dans le chemin de création de compte que vous avez indiqué dans la configuration du groupe de règles. Pour en savoir plus sur cette configuration, consultez Ajouter le groupe de règles géré par l'ACFP à votre ACL Web.

Si vous utilisez le groupe de règles `AWSManagedRulesATPRuleSet` géré, vous pouvez configurer un domaine qui correspond à celui indiqué dans le chemin de connexion que vous avez indiqué pour la configuration du groupe de règles. Pour en savoir plus sur cette configuration, consultez Ajouter le groupe de règles géré par ATP à votre ACL Web.

Utilisation de l' JavaScript API avec des politiques de sécurité du contenu

Si vous appliquez des politiques de sécurité du contenu (CSP) à vos ressources, pour que votre JavaScript implémentation fonctionne, vous devez autoriser le domaine AWS WAF apex sur la liste. `awswaf.com` Les JavaScript SDK appellent différents AWS WAF points de terminaison. Le fait d'autoriser la liste de ce domaine fournit les autorisations dont les SDK ont besoin pour fonctionner.

Voici un exemple de configuration permettant d'autoriser le domaine AWS WAF apex à être répertorié :

```
connect-src 'self' https://*.awswaf.com;
script-src 'self' https://*.awswaf.com;
script-src-elem 'self' https://*.awswaf.com;
```

Si vous essayez d'utiliser les JavaScript SDK avec des ressources utilisant le CSP et que vous n'avez pas autorisé le AWS WAF domaine, vous recevrez des erreurs du type suivant :

```
Refused to load the script ...awswaf.com/<> because it violates the following Content
 Security Policy directive: “script-src ‘self’
```

Utilisation de l' JavaScript API de gestion intelligente des menaces

Les API de menaces intelligentes fournissent des opérations permettant d'exécuter des défis silencieux contre le navigateur de l'utilisateur et de gérer les AWS WAF jetons qui prouvent le succès des réponses aux défis et aux CAPTCHA.

Implémentez l' JavaScript intégration d'abord dans un environnement de test, puis en production. Pour obtenir des conseils supplémentaires sur le codage, consultez les sections suivantes.

Pour utiliser les API de menaces intelligentes

1. Installation des API

   Si vous utilisez l'API CAPTCHA, vous pouvez ignorer cette étape. Lorsque vous installez l'API CAPTCHA, le script installe automatiquement les API de menaces intelligentes.

   a. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
   b. Dans le panneau de navigation, choisissez Intégration d'applications. Sur la page d'intégration des applications, vous pouvez voir les options sous forme d'onglets.
   c. Sélectionnez Intégration intelligente des menaces
   d. Dans l'onglet, sélectionnez l'ACL Web que vous souhaitez intégrer. La liste des ACL Web inclut uniquement les ACL Web qui utilisent le groupe de règles `AWSManagedRulesACFPRuleSet` `AWSManagedRulesATPRuleSet` géré, le groupe de règles géré ou le niveau de protection ciblé du groupe de règles `AWSManagedRulesBotControlRuleSet` géré.

e. Ouvrez le volet JavaScript SDK et copiez la balise de script à utiliser dans votre intégration.

f. Dans le code de page de votre application, dans la `<head>` section, insérez la balise de script que vous avez copiée pour l'ACL Web. Cette inclusion permet à votre application cliente de récupérer automatiquement un jeton en arrière-plan lors du chargement de la page.

```
<head>
    <script type="text/javascript" src="Web ACL integration URL/challenge.js”
 defer></script>
<head>
```

Cette `<script>` liste est configurée avec l'`defer`attribut, mais vous pouvez modifier le paramètre `async` si vous souhaitez un comportement différent pour votre page.

2. (Facultatif) Ajoutez une configuration de domaine pour les jetons du client : par défaut, AWS WAF lors de la création d'un jeton, celui-ci utilise le domaine hôte de la ressource associée à l'ACL Web. Pour fournir des domaines supplémentaires pour les JavaScript API, suivez les instructions surFournir des domaines à utiliser dans les jetons.

3. Codez votre intégration intelligente des menaces : écrivez votre code pour vous assurer que la récupération des jetons est terminée avant que le client n'envoie ses demandes à vos points de terminaison protégés. Si vous utilisez déjà l'`fetch`API pour effectuer votre appel, vous pouvez remplacer le `fetch` wrapper AWS WAF d'intégration. Si vous n'utilisez pas l'`fetch`API, vous pouvez utiliser l'`getToken`opération AWS WAF d'intégration à la place. Pour obtenir des conseils de codage, consultez les sections suivantes.

4. Ajoutez la vérification par jeton dans votre ACL Web — Ajoutez au moins une règle à votre ACL Web qui vérifie la validité d'un jeton de défi dans les requêtes Web envoyées par votre client. Vous pouvez utiliser des groupes de règles qui vérifient et surveillent les jetons de défi, comme le niveau cible du groupe de règles géré par Bot Control, et vous pouvez utiliser l'action de Challenge règle pour vérifier, comme décrit dansCAPTCHAet Challenge dans AWS WAF.

   Les ajouts à l'ACL Web vérifient que les demandes adressées à vos points de terminaison protégés incluent le jeton que vous avez acquis lors de l'intégration de votre client. Les demandes qui incluent un jeton valide et non expiré passent l'Challengeinspection et ne constituent pas un autre défi silencieux pour votre client.

5. (Facultatif) Bloquer les demandes pour lesquelles il manque des jetons — Si vous utilisez les API avec le groupe de règles géré par l'ACFP, le groupe de règles géré ATP ou les règles ciblées du groupe de règles Bot Control, ces règles ne bloquent pas les demandes contenant des jetons

manquants. Pour bloquer les demandes auxquelles il manque des jetons, suivez les instructions surBlocage des demandes dont le AWS WAF jeton n'est pas valide.

Rubriques

- Spécification de l'API de menace intelligente
- Comment utiliser le fetch wrapper d'intégration
- Comment utiliser l'intégration getToken

Spécification de l'API de menace intelligente

Cette section répertorie les spécifications relatives aux méthodes et aux propriétés des JavaScript API d'atténuation intelligente des menaces. Utilisez ces API pour intégrer des menaces intelligentes et des CAPTCHA.

`AwsWafIntegration.fetch()`

Envoie la `fetch` requête HTTP au serveur à l'aide de l'implémentation AWS WAF d'intégration.

`AwsWafIntegration.getToken()`

Récupère le AWS WAF jeton stocké et le stocke dans un cookie sur la page en cours avec un nom `aws-waf-token` et une valeur définie sur la valeur du jeton.

`AwsWafIntegration.hasToken()`

Renvoie une valeur booléenne indiquant si le `aws-waf-token` cookie contient actuellement un jeton non expiré.

Si vous utilisez également l'intégration CAPTCHA, consultez les spécifications correspondantes à l'adresse. Spécification de l'API CAPTCHA JavaScript

Comment utiliser le **`fetch`** wrapper d'intégration

Vous pouvez utiliser le AWS WAF `fetch` wrapper en modifiant vos `fetch` appels habituels à l'`fetch`API sous l'espace de `AwsWafIntegration` noms. Le AWS WAF wrapper prend en charge les mêmes options que l'appel d' JavaScript `fetch`API standard et ajoute la gestion des jetons pour l'intégration. Cette approche est généralement la méthode la plus simple pour intégrer votre application.

Avant l'implémentation du wrapper

La liste d'exemples suivante montre le code standard avant d'implémenter le `AwsWafIntegration fetch` wrapper.

```
const login_response = await fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

Après l'implémentation du wrapper

La liste suivante montre le même code avec l'implémentation du `AwsWafIntegration fetch` wrapper.

```
const login_response = await AwsWafIntegration.fetch(login_url, {
     method: 'POST',
     headers: {
       'Content-Type': 'application/json'
     },
     body: login_body
   });
```

Comment utiliser l'intégration **`getToken`**

AWS WAF nécessite que vos demandes adressées aux points de terminaison protégés incluent le cookie nommé `aws-waf-token` avec la valeur de votre jeton actuel.

L'`getToken`opération est un appel d'API asynchrone qui récupère le AWS WAF jeton et le stocke dans un cookie sur la page en cours avec un nom `aws-waf-token` et une valeur définie sur la valeur du jeton. Vous pouvez utiliser ce cookie symbolique selon vos besoins sur votre page.

Lorsque vous appelez`getToken`, il effectue les opérations suivantes :

- Si un jeton non expiré est déjà disponible, l'appel le renvoie immédiatement.
- Dans le cas contraire, l'appel récupère un nouveau jeton auprès du fournisseur de jetons, en attendant jusqu'à 2 secondes que le flux de travail d'acquisition de jetons soit terminé avant l'expiration du délai imparti. Si l'opération expire, elle génère une erreur que votre code d'appel doit gérer.

L'`getToken`opération est accompagnée d'une `hasToken` opération qui indique si le `aws-waf-token` cookie contient actuellement un jeton non expiré.

`AwsWafIntegration.getToken()`récupère un jeton valide et le stocke sous forme de cookie. La plupart des appels clients joignent automatiquement ce cookie, mais ce n'est pas le cas pour certains. Par exemple, les appels passés entre des domaines hôtes ne joignent pas le cookie. Dans les détails de mise en œuvre qui suivent, nous montrons comment travailler avec les deux types d'appels clients.

`getToken`Implémentation de base, pour les appels qui joignent le **`aws-waf-token`** cookie

L'exemple de liste suivant montre le code standard pour implémenter l'`getToken`opération avec une demande de connexion.

```
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
 }
```

Soumettre le formulaire uniquement une fois que le jeton sera disponible auprès de **`getToken`**

La liste suivante indique comment enregistrer un écouteur d'événements pour intercepter les soumissions de formulaires jusqu'à ce qu'un jeton valide soit disponible pour utilisation.

```
<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>
```

Joindre le jeton lorsque votre client n'attache pas le **`aws-waf-token`** cookie par défaut

`AwsWafIntegration.getToken()`récupère un jeton valide et le stocke sous forme de cookie, mais tous les appels clients ne joignent pas ce cookie par défaut. Par exemple, les appels passés entre des domaines hôtes ne joignent pas le cookie.

Le `fetch` wrapper gère ces cas automatiquement, mais si vous n'êtes pas en mesure d'utiliser le `fetch` wrapper, vous pouvez le faire en utilisant un en-tête personnalisé`x-aws-waf-token`. AWS WAF lit les jetons depuis cet en-tête, en plus de les lire depuis le `aws-waf-token` cookie. Le code suivant montre un exemple de définition de l'en-tête.

```
const token = await AwsWafIntegration.getToken();
const result = await fetch('/url', {
    headers: {
        'x-aws-waf-token': token,
    },
});
```

Par défaut, AWS WAF n'accepte que les jetons contenant le même domaine que le domaine hôte demandé. Tous les jetons interdomaines nécessitent des entrées correspondantes dans la liste des domaines des jetons ACL Web. Pour plus d'informations, consultez AWS WAF configuration de la liste de domaines du jeton ACL Web.

Pour plus d'informations sur l'utilisation de jetons entre domaines, consultez aws-waf-bot-controlaws-samples/ -. api-protection-with-captcha

Utilisation de l'API CAPTCHA JavaScript

L' JavaScript API CAPTCHA vous permet de configurer le puzzle CAPTCHA et de le placer où vous le souhaitez dans votre application cliente. Cette API exploite les fonctionnalités des API de menaces intelligentes pour acquérir et utiliser JavaScript des AWS WAF jetons une fois qu'un utilisateur final a réussi à résoudre un casse-tête CAPTCHA.

Implémentez l' JavaScript intégration d'abord dans un environnement de test, puis en production. Pour obtenir des conseils supplémentaires sur le codage, consultez les sections suivantes.

Pour utiliser l'API d'intégration CAPTCHA

1. Installation de l'API

   a. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
   b. Dans le panneau de navigation, choisissez Intégration d'applications. Sur la page d'intégration des applications, vous pouvez voir les options sous forme d'onglets.
   c. Sélectionnez l'intégration CAPTCHA.
   d. Copiez la balise de script JavaScript d'intégration répertoriée pour l'utiliser dans votre intégration.
   e. Dans le code de page de votre application, dans la `<head>` section, insérez la balise de script que vous avez copiée. Cette inclusion rend le puzzle CAPTCHA disponible pour la configuration et l'utilisation.

      ```
      <head>
          <script type="text/javascript" src="integrationURL/jsapi.js" defer></
      script>
      </head>
      ```

      Cette `<script>` liste est configurée avec l'`defer`attribut, mais vous pouvez modifier le paramètre `async` si vous souhaitez un comportement différent pour votre page.

      Le script CAPTCHA charge également automatiquement le script d'intégration intelligente des menaces s'il n'est pas déjà présent. Le script intelligent d'intégration des menaces permet à votre application cliente de récupérer automatiquement un jeton en arrière-plan

lors du chargement de la page et fournit d'autres fonctionnalités de gestion des jetons dont vous avez besoin pour utiliser l'API CAPTCHA.

2. (Facultatif) Ajoutez une configuration de domaine pour les jetons du client : par défaut, AWS WAF lors de la création d'un jeton, celui-ci utilise le domaine hôte de la ressource associée à l'ACL Web. Pour fournir des domaines supplémentaires pour les JavaScript API, suivez les instructions surFournir des domaines à utiliser dans les jetons.
3. Obtenir la clé d'API cryptée pour le client — L'API CAPTCHA nécessite une clé d'API cryptée contenant une liste de domaines clients valides. AWS WAF utilise cette clé pour vérifier que le domaine client que vous utilisez avec l'intégration est approuvé pour utiliser le AWS WAF CAPTCHA. Pour générer votre clé d'API, suivez les instructions surGestion des clés d'API pour l'API JS CAPTCHA.
4. Codez l'implémentation de votre widget CAPTCHA : implémentez l'appel d'`renderCaptcha()`API sur votre page, à l'endroit où vous souhaitez l'utiliser. Pour plus d'informations sur la configuration et l'utilisation de cette fonction, consultez les sections suivantes, Spécification de l'API CAPTCHA JavaScript etComment afficher le casse-tête CAPTCHA.

   L'implémentation du CAPTCHA s'intègre aux API d'intégration intelligente des menaces pour la gestion des jetons et pour exécuter des appels de récupération utilisant les jetons. AWS WAF Pour obtenir des conseils sur l'utilisation de ces API, consultezUtilisation de l' JavaScript API de gestion intelligente des menaces.
5. Ajoutez la vérification par jeton dans votre ACL Web — Ajoutez au moins une règle à votre ACL Web qui vérifie la validité d'un jeton CAPTCHA dans les requêtes Web envoyées par votre client. Vous pouvez utiliser l'action de CAPTCHA règle pour vérifier, comme décrit dansCAPTCHAet Challenge dans AWS WAF.

   Les ajouts à l'ACL Web vérifient que les demandes adressées à vos points de terminaison protégés incluent le jeton que vous avez acquis lors de l'intégration de votre client. Les demandes qui incluent un jeton CAPTCHA valide et non expiré passent l'inspection des CAPTCHA règles et ne présentent aucun autre casse-tête CAPTCHA à votre utilisateur final.

Rubriques

- Spécification de l'API CAPTCHA JavaScript
- Comment afficher le casse-tête CAPTCHA
- Gestion d'une réponse CAPTCHA depuis AWS WAF

- Gestion des clés d'API pour l'API JS CAPTCHA

Spécification de l'API CAPTCHA JavaScript

Cette section répertorie les spécifications relatives aux méthodes et aux propriétés des API CAPTCHA JavaScript . Utilisez les JavaScript API CAPTCHA pour exécuter des puzzles CAPTCHA personnalisés dans vos applications clientes.

Cette API s'appuie sur les API de menaces intelligentes, que vous utilisez pour configurer et gérer l'acquisition et l'utilisation de AWS WAF jetons. VoirSpécification de l'API de menace intelligente.

`AwsWafCaptcha.renderCaptcha(container, configuration)`

Présente un casse-tête AWS WAF CAPTCHA à l'utilisateur final et, en cas de succès, met à jour le jeton client avec la validation CAPTCHA. Ceci n'est disponible qu'avec l'intégration CAPTCHA. Utilisez cet appel ainsi que les API de menaces intelligentes pour gérer la récupération des jetons et pour fournir le jeton dans vos `fetch` appels. Consultez les API de menaces intelligentes à l'adresseSpécification de l'API de menace intelligente.

Contrairement à l'interstitiel CAPTCHA qui AWS WAF envoie, le puzzle CAPTCHA rendu par cette méthode affiche le puzzle immédiatement, sans écran de titre initial.

`container`

L'`Element`objet de l'élément conteneur cible sur la page. Ceci est généralement récupéré en appelant `document.getElementById()` ou`document.querySelector()`.

Obligatoire : oui

Type : `Element`

configuration

Un objet contenant les paramètres de configuration CAPTCHA, comme suit :

`apiKey`

La clé API cryptée qui autorise les autorisations pour le domaine du client. Utilisez la AWS WAF console pour générer vos clés d'API pour les domaines de vos clients. Vous pouvez utiliser une clé pour un maximum de cinq domaines. Pour plus d’informations, consultez Gestion des clés d'API pour l'API JS CAPTCHA.

Obligatoire : oui

Type : `string`

`onSuccess: (wafToken: string) => void;`

Appelé avec un AWS WAF jeton valide lorsque l'utilisateur final termine avec succès un casse-tête CAPTCHA. Utilisez le jeton dans les demandes que vous envoyez aux points de terminaison que vous protégez avec une ACL AWS WAF Web. Le jeton fournit la preuve et l'horodatage de la dernière réalisation réussie du puzzle.

Obligatoire : oui

`onError?: (error: CaptchaError) => void;`

Appelé avec un objet d'erreur lorsqu'une erreur survient lors de l'opération CAPTCHA.

Obligatoire : non

`CaptchaError`définition de classe — Le `onError` gestionnaire fournit un type d'erreur avec la définition de classe suivante.

```
CaptchaError extends Error {
    kind: "internal_error" | "network_error" | "token_error" | "client_error";
    statusCode?: number;
}
```

- `kind`— Le type d'erreur renvoyé.
- `statusCode`— Le code d'état HTTP, s'il est disponible. Ceci est utilisé `network_error` si l'erreur est due à une erreur HTTP.

`onLoad?: () => void;`

Appelé lors du chargement d'un nouveau casse-tête CAPTCHA.

Obligatoire : non

`onPuzzleTimeout?: () => void;`

Appelé lorsqu'un casse-tête CAPTCHA n'est pas terminé avant son expiration.

Obligatoire : non

`onPuzzleCorrect?: () => void;`

Appelé lorsqu'une réponse correcte est fournie à un casse-tête CAPTCHA.

Obligatoire : non

`onPuzzleIncorrect?: () => void;`

Appelé lorsqu'une réponse incorrecte est fournie à un casse-tête CAPTCHA.

Obligatoire : non

`defaultLocale`

La localisation par défaut à utiliser pour le puzzle CAPTCHA. Les instructions écrites pour les puzzles CAPTCHA sont disponibles en arabe (ar-SA), chinois simplifié (zh-CN), néerlandais (nl-NL), anglais (en-US), français (fr-FR), allemand (de-DE), italien (it-IT), japonais (ja-JP), portugais brésilien (pT-BR), espagnol (es-ES) et turc (tr-TR). Les instructions audio sont disponibles pour toutes les langues écrites, à l'exception du chinois et du japonais, qui sont par défaut l'anglais. Pour modifier la langue par défaut, fournissez la langue internationale et le code local, par exemple,`ar-SA`.

Par défaut : langue actuellement utilisée dans le navigateur de l'utilisateur final

Obligatoire : non

Type : `string`

`disableLanguageSelector`

S'il est défini sur`true`, le casse-tête CAPTCHA masque le sélecteur de langue.

Par défaut: `false`

Obligatoire : non

Type : `boolean`

`dynamicWidth`

S'il est défini sur`true`, le puzzle CAPTCHA change de largeur pour être compatible avec la largeur de la fenêtre du navigateur.

Par défaut: `false`

Obligatoire : non

Type : `boolean`

`skipTitle`

S'il est défini sur`true`, le casse-tête CAPTCHA n'affiche pas le titre du puzzle intitulé Résoudre le puzzle.

Par défaut: `false`

Obligatoire : non

Type : `boolean`

Comment afficher le casse-tête CAPTCHA

Vous pouvez utiliser l' AWS WAF `renderCaptcha`appel où vous le souhaitez dans votre interface client. L'appel permet de récupérer un casse-tête CAPTCHA AWS WAF, de le restituer et d'envoyer les résultats à des fins de vérification. AWS WAF Lorsque vous passez l'appel, vous indiquez la configuration du rendu du puzzle et les rappels que vous souhaitez exécuter lorsque vos utilisateurs finaux auront terminé le puzzle. Pour plus de détails sur les options, reportez-vous à la section précédente,Spécification de l'API CAPTCHA JavaScript .

Utilisez cet appel conjointement avec la fonctionnalité de gestion des jetons des API d'intégration intelligente des menaces. Cet appel fournit à votre client un jeton qui vérifie la réussite du casse-tête CAPTCHA. Utilisez les API d'intégration intelligente des menaces pour gérer le jeton et pour fournir le jeton dans les appels de votre client aux points de terminaison protégés par des ACL AWS WAF Web. Pour plus d'informations sur les API de menaces intelligentes, consultezUtilisation de l' JavaScript API de gestion intelligente des menaces.

Exemple de mise en œuvre

La liste d'exemples suivante montre une implémentation CAPTCHA standard, y compris le placement de l'URL d' AWS WAF intégration dans la <head> section.

Cette liste configure la `renderCaptcha` fonction avec un rappel de réussite qui utilise le `AwsWafIntegration.fetch` wrapper des API d'intégration intelligente des menaces. Pour plus d'informations sur cette fonction, consultezComment utiliser le `fetch` wrapper d'intégration.

```
<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>
```

Exemples de paramètres de configuration

L'exemple de liste suivant montre les `renderCaptcha` paramètres autres que ceux par défaut pour les options de largeur et de titre.

```
        AwsWafCaptcha.renderCaptcha(container, {
            apiKey: "...API key goes here...",
            onSuccess: captchaExampleSuccessFunction,
            onError: captchaExampleErrorFunction,
            dynamicWidth: true,
```

```
            skipTitle: true
        });
```

Pour obtenir des informations complètes sur les options de configuration, consultezSpécification de l'API CAPTCHA JavaScript .

Gestion d'une réponse CAPTCHA depuis AWS WAF

Une AWS WAF règle comportant une CAPTCHA action met fin à l'évaluation d'une requête Web correspondante si celle-ci ne contient pas de jeton avec un horodatage CAPTCHA valide. Si la demande est un appel `GET` text/html, l'CAPTCHAaction envoie alors au client un interstitiel contenant un casse-tête CAPTCHA. Lorsque vous n'intégrez pas l' JavaScript API CAPTCHA, l'interstitiel exécute le puzzle et, si l'utilisateur final le résout avec succès, soumet automatiquement à nouveau la demande.

Lorsque vous intégrez l' JavaScript API CAPTCHA et que vous personnalisez votre gestion des CAPTCHA, vous devez détecter la réponse CAPTCHA finale, fournir votre CAPTCHA personnalisé, puis si l'utilisateur final résout le casse-tête avec succès, soumettre à nouveau la demande Web du client.

L'exemple de code suivant montre comment procéder :

> **Note**
>
> La réponse à l' AWS WAF CAPTCHAaction possède un code d'état HTTP 405, que nous utilisons pour reconnaître la CAPTCHA réponse dans ce code. Si votre point de terminaison protégé utilise un code d'état HTTP 405 pour communiquer tout autre type de réponse pour le même appel, cet exemple de code affichera également un casse-tête CAPTCHA pour ces réponses.

```
<!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>
```

Gestion des clés d'API pour l'API JS CAPTCHA

Pour intégrer le AWS WAF CAPTCHA dans une application cliente avec l' JavaScript API, vous avez besoin de la balise d'intégration d' JavaScript API et de la clé d'API cryptée pour le domaine client dans lequel vous souhaitez exécuter votre puzzle CAPTCHA.

L'intégration de l'application CAPTCHA JavaScript utilise les clés d'API cryptées pour vérifier que le domaine de l'application client est autorisé à utiliser l'API AWS WAF CAPTCHA. Lorsque vous appelez l'API CAPTCHA depuis votre JavaScript client, vous fournissez une clé d'API avec une liste de domaines qui inclut un domaine pour le client actuel. Vous pouvez répertorier jusqu'à 5 domaines dans une seule clé cryptée.

Exigences clés de l'API

La clé d'API que vous utilisez dans votre intégration CAPTCHA doit contenir un domaine qui s'applique au client sur lequel vous utilisez la clé.

- Si vous spécifiez un `window.awsWafCookieDomainList` dans l'intégration intelligente des menaces de votre client, au moins un domaine de votre clé d'API doit correspondre exactement à l'un des domaines de jetons `window.awsWafCookieDomainList` ou doit être le domaine apex de l'un de ces domaines de jetons.

  Par exemple, pour le domaine de jeton`mySubdomain.myApex.com`, la clé `mySubdomain.myApex.com` d'API correspond exactement et la clé d'API `myApex.com` est le domaine apex. L'une ou l'autre des clés correspond au domaine du jeton.

  Pour plus d'informations sur le paramétrage de la liste des domaines de jetons, consultezFournir des domaines à utiliser dans les jetons.
- Dans le cas contraire, le domaine actuel doit être contenu dans la clé d'API. Le domaine actuel est celui que vous pouvez voir dans la barre d'adresse du navigateur.

Les domaines que vous utilisez doivent être ceux qui AWS WAF seront acceptés, en fonction du domaine hôte protégé et de la liste de domaines de jetons configurée pour l'ACL Web. Pour plus d'informations, consultez AWS WAF configuration de la liste de domaines du jeton ACL Web.

Comment choisir la région pour votre clé d'API

AWS WAF peut générer des clés d'API CAPTCHA dans toutes les régions où elles AWS WAF sont disponibles.

En règle générale, vous devez utiliser la même région pour votre clé d'API CAPTCHA que celle que vous utilisez pour votre ACL Web. Toutefois, si vous vous attendez à une audience mondiale pour une ACL Web régionale, vous pouvez obtenir une balise d' JavaScript intégration CAPTCHA limitée CloudFront et une clé d'API limitée à CloudFront, et les utiliser avec une ACL Web régionale. Cette

approche permet aux clients de charger un casse-tête CAPTCHA depuis la région la plus proche d'eux, ce qui réduit le temps de latence.

Les clés d'API CAPTCHA qui sont limitées à des régions autres que ne CloudFront sont pas prises en charge pour une utilisation dans plusieurs régions. Ils ne peuvent être utilisés que dans la région à laquelle ils sont destinés.

Pour générer une clé d'API pour les domaines de vos clients

Pour obtenir l'URL d'intégration et générer et récupérer les clés d'API via la console.

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le panneau de navigation, choisissez Intégration d'applications.
3. Dans le volet, les ACL Web activées pour l'intégration des applications, sélectionnez la région que vous souhaitez utiliser pour votre clé d'API. Vous pouvez également sélectionner la région dans le volet des clés d'API de l'onglet d'intégration CAPTCHA.
4. Choisissez l'onglet Intégration CAPTCHA. Cet onglet fournit la balise d' JavaScript intégration CAPTCHA, que vous pouvez utiliser dans votre intégration, ainsi que la liste des clés d'API. Les deux sont limités à la région sélectionnée.
5. Dans le volet des clés d'API, choisissez Generate key. Le dialogue de génération de clés apparaît.
6. Entrez les domaines clients que vous souhaitez inclure dans la clé. Vous pouvez saisir jusqu'à 5. Lorsque vous avez terminé, choisissez Generate key. L'interface revient à l'onglet d'intégration CAPTCHA, où votre nouvelle clé est répertoriée.

   Une fois créée, une clé d'API est immuable. Si vous devez apporter des modifications à une clé, générez une nouvelle clé et utilisez-la à la place.
7. (Facultatif) Copiez la clé nouvellement générée pour l'utiliser dans votre intégration.

Vous pouvez également utiliser les API REST ou l'un des AWS SDK spécifiques au langage pour ce travail. Les appels d'API REST sont CreateApiKey et ListApiKeys.

Pour supprimer une clé d'API

Pour supprimer une clé d'API, vous devez utiliser l'API REST ou l'un des AWS SDK spécifiques au langage. L'appel de l'API REST est DeleteApiKey. Vous ne pouvez pas utiliser la console pour supprimer une clé.

Après avoir supprimé une clé, cela peut prendre jusqu'à 24 heures AWS WAF pour interdire son utilisation dans toutes les régions.

AWS WAF intégration d'applications mobiles

Vous pouvez utiliser les SDK AWS WAF mobiles pour implémenter des SDK d'intégration AWS WAF intelligente des menaces pour les applications mobiles Android et iOS.

- Pour les applications mobiles Android, les AWS WAF SDK fonctionnent pour l'API Android version 23 (Android version 6) et versions ultérieures. Pour plus d'informations sur les versions d'Android, consultez les notes de mise à jour de SDK Platform.
- Pour les applications mobiles iOS, AWS WAF les SDK fonctionnent pour iOS version 13 et versions ultérieures. Pour plus d'informations sur les versions d'iOS, consultez les notes de mise à jour pour iOS et iPadOS.

Avec le SDK mobile, vous pouvez gérer l'autorisation des jetons et inclure les jetons dans les demandes que vous envoyez à vos ressources protégées. En utilisant les SDK, vous vous assurez que ces appels de procédure à distance effectués par votre client contiennent un jeton valide. En outre, lorsque cette intégration est en place sur les pages de votre application, vous pouvez implémenter des règles d'atténuation dans votre ACL Web, telles que le blocage des demandes qui ne contiennent pas de jeton valide.

Pour accéder aux SDK mobiles, contactez l'assistance via Contact AWS.

> **Note**
>
> Les SDK AWS WAF mobiles ne sont pas disponibles pour la personnalisation du CAPTCHA.

L'approche de base pour utiliser le SDK consiste à créer un fournisseur de jetons à l'aide d'un objet de configuration, puis à utiliser le fournisseur de jetons pour récupérer des AWS WAF jetons. Par défaut, le fournisseur de jetons inclut les jetons récupérés dans vos requêtes Web adressées à votre ressource protégée.

Voici une liste partielle d'une implémentation du SDK, qui montre les principaux composants. Pour obtenir des exemples détaillés, consultez Écrire votre code pour le SDK AWS WAF mobile.

iOS

```
let url: URL = URL(string: "Web ACL integration URL")!
 let configuration = WAFConfiguration(applicationIntegrationUrl: url, domainName:
 "Domain name")
 let tokenProvider = WAFTokenProvider(configuration)
 let token = tokenProvider.getToken()
```

Android

```
URL applicationIntegrationURL = new URL("Web ACL integration URL");
 String domainName = "Domain name";
 WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
 WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);
 WAFToken token = tokenProvider.getToken();
```

Installation du SDK AWS WAF mobile

Pour accéder aux SDK mobiles, contactez l'assistance via Contact AWS.

Implémentez le SDK mobile d'abord dans un environnement de test, puis en production.

Pour installer le SDK AWS WAF mobile

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le panneau de navigation, choisissez Intégration d'applications.
3. Dans l'onglet Intégrations intelligentes des menaces, procédez comme suit :

    a. Dans le volet ACL Web activées pour l'intégration des applications, localisez l'ACL Web à laquelle vous procédez à l'intégration. Copiez et enregistrez l'URL d'intégration Web ACL à utiliser dans votre implémentation. Vous pouvez également obtenir cette URL via l'appel d'API`GetWebACL`.

    b. Choisissez le type et la version de l'appareil mobile, puis choisissez Télécharger. Vous pouvez choisir la version de votre choix, mais nous vous recommandons d'utiliser la

dernière version. AWS WAF télécharge le `zip` fichier pour votre appareil sur votre emplacement de téléchargement standard.

4. Dans votre environnement de développement d'applications, décompressez le fichier sur l'emplacement de travail de votre choix. Dans le répertoire de premier niveau du fichier zip, recherchez et ouvrez le`README`. Suivez les instructions du `README` fichier pour installer le SDK AWS WAF mobile à utiliser dans le code de votre application mobile.
5. Programmez votre application conformément aux instructions des sections suivantes.

Spécification du SDK AWS WAF mobile

Cette section répertorie les objets du SDK, les opérations et les paramètres de configuration de la dernière version disponible du SDK AWS WAF mobile. Pour des informations détaillées sur le fonctionnement du fournisseur de jetons et des opérations pour les différentes combinaisons de paramètres de configuration, consultezFonctionnement du SDK AWS WAF mobile.

`WAFToken`

Détient un AWS WAF jeton.

`getValue()`

Récupère la `String` représentation du. `WAFToken`

`WAFTokenProvider`

Gère les jetons dans votre application mobile. Implémentez cela à l'aide d'un `WAFConfiguration` objet.

`getToken()`

Si l'actualisation en arrière-plan est activée, le jeton mis en cache est renvoyé. Si l'actualisation en arrière-plan est désactivée, un appel synchrone bloquant est lancé AWS WAF pour récupérer un nouveau jeton.

`onTokenReady(WAFTokenResultCallback)`

Demande au fournisseur de jetons d'actualiser le jeton et d'invoquer le rappel fourni lorsqu'un jeton actif est prêt. Le fournisseur de jetons invoquera votre rappel dans un fil d'arrière-plan lorsque le jeton sera mis en cache et prêt. Appelez cela lorsque votre application se charge pour la première fois et également lorsqu'elle revient à un état actif. Pour plus d'informations sur le retour à un état actif, consultezthe section called “Récupération d'un jeton suite à l'inactivité d'une application”.

Pour les applications Android ou iOS, vous pouvez `WAFTokenResultCallback` définir l'opération que vous souhaitez que le fournisseur de jetons appelle lorsqu'un jeton demandé est prêt. Votre implémentation de `WAFTokenResultCallback` doit prendre les paramètres`WAFToken`,`SdkError`. Pour les applications iOS, vous pouvez également créer une fonction intégrée.

`storeTokenInCookieStorage(WAFToken)`

Indique au `WAFTokenProvider` de stocker le AWS WAF jeton spécifié dans le gestionnaire de cookies du SDK. Par défaut, le jeton n'est ajouté au magasin de cookies que lorsqu'il est acquis pour la première fois et lorsqu'il est actualisé. Si l'application efface le magasin de cookies partagé pour une raison quelconque, le SDK n'ajoute pas automatiquement le AWS WAF jeton avant la prochaine actualisation.

`WAFConfiguration`

Détient la configuration pour la mise en œuvre du`WAFTokenProvider`. Lorsque vous implémentez cela, vous fournissez l'URL d'intégration de votre ACL Web, le nom de domaine à utiliser dans le jeton et tous les paramètres autres que ceux par défaut que vous souhaitez que le fournisseur de jetons utilise.

La liste suivante indique les paramètres de configuration que vous pouvez gérer dans l'`WAFConfiguration`objet.

`applicationIntegrationUrl`

URL d'intégration de l'application. Obtenez-le depuis la AWS WAF console ou via l'appel `getWebACL` d'API.

Obligatoire : oui

Type : URL spécifique à l'application. Pour iOS, voir URL iOS. Pour Android, consultez l'URL java.net.

`backgroundRefreshEnabled`

Indique si vous souhaitez que le fournisseur de jetons actualise le jeton en arrière-plan. Si vous définissez cette option, le fournisseur de jetons actualise vos jetons en arrière-plan conformément aux paramètres de configuration qui régissent les activités d'actualisation automatique des jetons.

Obligatoire : non

Type : `Boolean`

Valeur par défaut : `TRUE`

`domainName`

Le domaine à utiliser dans le jeton, qui est utilisé pour l'acquisition de jetons et le stockage des cookies. Par exemple, `example.com` ou `aws.amazon.com`. Il s'agit généralement du domaine hôte de votre ressource associé à l'ACL Web, dans lequel vous allez envoyer des requêtes Web. Pour le groupe de règles géré par l'ACFP`AWSManagedRulesACFPRuleSet`, il s'agit généralement d'un domaine unique correspondant au domaine indiqué dans le chemin de création de compte que vous avez indiqué dans la configuration du groupe de règles. Pour le groupe de règles géré par ATP`AWSManagedRulesATPRuleSet`, il s'agit généralement d'un domaine unique correspondant au domaine indiqué dans le chemin de connexion que vous avez indiqué dans la configuration du groupe de règles.

Les suffixes publics ne sont pas autorisés. Par exemple, vous ne pouvez pas utiliser `gov.au` ou `co.uk` comme domaine de jeton.

Le domaine doit être accepté, sur la base du domaine hôte protégé et de la liste des domaines de jetons de l'ACL Web. AWS WAF Pour plus d'informations, consultez AWS WAF configuration de la liste de domaines du jeton ACL Web.

Obligatoire : oui

Type : `String`

`maxErrorTokenRefreshDelayMsec`

Durée maximale en millisecondes d'attente avant de répéter l'actualisation d'un jeton après une tentative infructueuse. Cette valeur est utilisée après l'échec de la récupération du jeton et après plusieurs tentatives`maxRetryCount`.

Obligatoire : non

Type : `Integer`

Valeur par défaut : `5000` (5 secondes)

Valeur minimale autorisée : `1` (1 milliseconde)

Valeur maximale autorisée : `30000` (30 secondes)

`maxRetryCount`

Nombre maximal de tentatives à effectuer avec un retard exponentiel lorsqu'un jeton est demandé.

Obligatoire : non

Type : `Integer`

Valeur par défaut : Si l'actualisation de l'arrière-plan est activée,`5`. Sinon la valeur est renvoy, `3`.

Valeur minimale autorisée : `0`

Valeur maximale autorisée : `10`

`setTokenCookie`

Indique si vous souhaitez que le gestionnaire de cookies du SDK ajoute un cookie jeton à vos demandes. Par défaut, cela ajoute un cookie symbolique à toutes les demandes. Le gestionnaire de cookies ajoute un cookie jeton à toute demande dont le chemin est inférieur au chemin spécifié dans`tokenCookiePath`.

Obligatoire : non

Type : `Boolean`

Valeur par défaut : `TRUE`

`tokenCookiePath`

Utilisé quand `setTokenCookie` c'est le cas`TRUE`. Indique le chemin de niveau supérieur où vous souhaitez que le gestionnaire de cookies du SDK ajoute un cookie jeton. Le gestionnaire ajoute un cookie symbolique à toutes les demandes que vous envoyez à ce chemin et à tous les chemins enfants.

Par exemple, si vous définissez ce paramètre sur`/web/login`, le gestionnaire inclut le cookie jeton pour tout ce qui est envoyé `/web/login` et pour tous ses chemins enfants, par exemple`/web/login/help`. Il n'inclut pas le jeton pour les demandes envoyées vers d'autres chemins`/`, comme`/web`, ou`/web/order`.

Obligatoire : non

Type : `String`

Valeur par défaut : `/`

`tokenRefreshDelaySec`

Utilisé pour le rafraîchissement de l'arrière-plan. Durée maximale en secondes entre les actualisations du jeton d'arrière-plan.

Obligatoire : non

Type : `Integer`

Valeur par défaut : 88

Valeur minimale autorisée : 88

Valeur maximale autorisée : `300` (5 minutes)

Fonctionnement du SDK AWS WAF mobile

Les SDK mobiles vous fournissent un fournisseur de jetons configurable que vous pouvez utiliser pour récupérer et utiliser des jetons. Le fournisseur de jetons vérifie que les demandes que vous autorisez proviennent de clients légitimes. Lorsque vous envoyez des demandes aux AWS ressources que vous protégez AWS WAF, vous incluez le jeton dans un cookie afin de valider la demande. Vous pouvez gérer le cookie de jeton manuellement ou demander au fournisseur de jetons de le faire pour vous.

Cette section couvre les interactions entre les classes, les propriétés et les méthodes incluses dans le SDK mobile. Pour les spécifications du SDK, voirSpécification du SDK AWS WAF mobile.

Récupération et mise en cache des jetons

Lorsque vous créez l'instance du fournisseur de jetons dans votre application mobile, vous configurez la manière dont vous souhaitez qu'elle gère les jetons et leur récupération. Votre principal choix est de savoir comment conserver des jetons valides et non expirés à utiliser dans les requêtes Web de votre application :

- Actualisation de l'arrière-plan activée : il s'agit de la valeur par défaut. Le fournisseur de jetons actualise automatiquement le jeton en arrière-plan et le met en cache. Lorsque l'actualisation en arrière-plan est activée, lorsque vous appelez`getToken()`, l'opération récupère le jeton mis en cache.

Le fournisseur de jetons effectue l'actualisation du jeton à des intervalles configurables, de sorte qu'un jeton non expiré soit toujours disponible dans le cache lorsque l'application est active. L'actualisation en arrière-plan est suspendue lorsque votre application est inactive. Pour plus d'informations à ce sujet, consultezRécupération d'un jeton suite à l'inactivité d'une application.

- Actualisation en arrière-plan désactivée : vous pouvez désactiver l'actualisation des jetons en arrière-plan, puis récupérer les jetons uniquement sur demande. Les jetons récupérés à la demande ne sont pas mis en cache et vous pouvez en récupérer plusieurs si vous le souhaitez. Chaque jeton est indépendant des autres que vous récupérez, et chacun possède son propre horodatage utilisé pour calculer l'expiration.

  Les options suivantes s'offrent à vous pour récupérer les jetons lorsque l'actualisation en arrière-plan est désactivée :

  - **`getToken()`**— Lorsque vous appelez `getToken()` avec l'actualisation en arrière-plan désactivée, l'appel récupère de manière synchrone un nouveau jeton depuis. AWS WAF Il s'agit d'un appel potentiellement bloquant qui peut affecter la réactivité de l'application si vous l'invoquez sur le thread principal.
  - **`onTokenReady(WAFTokenResultCallback)`**— Cet appel récupère un nouveau jeton de manière asynchrone, puis invoque le rappel du résultat fourni dans un thread d'arrière-plan lorsqu'un jeton est prêt.

Comment le fournisseur de jetons tente à nouveau de récupérer un jeton qui a échoué

Le fournisseur de jetons réessaie automatiquement de récupérer le jeton en cas d'échec de la récupération. Les nouvelles tentatives sont initialement effectuées à l'aide d'une temporisation exponentielle avec un temps d'attente de départ de 100 ms. Pour plus d'informations sur les tentatives exponentielles, reportez-vous à la section Rétentatives d'erreur et recul exponentiel dans. AWS

Lorsque le nombre de tentatives atteint le nombre configuré`maxRetryCount`, le fournisseur de jetons arrête d'essayer ou passe à essayer toutes les `maxErrorTokenRefreshDelayMsec` millisecondes, selon le type de récupération du jeton :

- **`onTokenReady()`**— Le fournisseur de jetons passe à l'attente de quelques `maxErrorTokenRefreshDelayMsec` millisecondes entre les tentatives et continue d'essayer de récupérer le jeton.

- Actualisation en arrière-plan : le fournisseur de jetons passe à l'attente de quelques `maxErrorTokenRefreshDelayMsec` millisecondes entre les tentatives et continue d'essayer de récupérer le jeton.
- **`getToken()`**Appels à la demande, lorsque l'actualisation en arrière-plan est désactivée : le fournisseur de jetons arrête d'essayer de récupérer un jeton et renvoie la valeur du jeton précédent, ou une valeur nulle s'il n'existe aucun jeton précédent.

Récupération d'un jeton suite à l'inactivité d'une application

L'actualisation en arrière-plan n'est effectuée que lorsque votre application est considérée comme active pour votre type d'application :

- iOS — L'actualisation de l'arrière-plan est effectuée lorsque l'application est au premier plan.
- Android — L'actualisation de l'arrière-plan est effectuée lorsque l'application n'est pas fermée, qu'elle soit au premier plan ou en arrière-plan.

Si votre application reste dans un état qui ne prend pas en charge l'actualisation en arrière-plan pendant plus de `tokenRefreshDelaySec` quelques secondes que vous avez configurées, le fournisseur de jetons interrompt l'actualisation en arrière-plan. Par exemple, pour une application iOS, si la valeur `tokenRefreshDelaySec` est 300 et que l'application se ferme ou passe en arrière-plan pendant plus de 300 secondes, le fournisseur de jetons arrête d'actualiser le jeton. Lorsque l'application revient à un état actif, le fournisseur de jetons redémarre automatiquement l'actualisation en arrière-plan.

Lorsque votre application revient à un état actif, appelez `onTokenReady()` pour être averti lorsque le fournisseur de jetons a récupéré et mis en cache un nouveau jeton. Ne vous contentez pas d'appeler`getToken()`, car le cache ne contient peut-être pas encore de jeton valide et actuel.

Écrire votre code pour le SDK AWS WAF mobile

Cette section fournit des exemples de code pour l'utilisation du SDK mobile.

Initialisation du fournisseur de jetons et obtention de jetons

Vous lancez votre instance de fournisseur de jetons à l'aide d'un objet de configuration. Vous pouvez ensuite récupérer des jetons en utilisant les opérations disponibles. Les éléments de base du code requis sont présentés ci-dessous.

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

Exemple Java :

```
String applicationIntegrationURL = "Web ACL integration URL";
//Or
URL applicationIntegrationURL = new URL("Web ACL integration URL");

String domainName = "Domain name";

WAFConfiguration configuration =
 WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL).domainName(
WAFTokenProvider tokenProvider = new WAFTokenProvider(Application context,
 configuration);

// implement a token result callback
WAFTokenResultCallback callback = (wafToken, error) -> {
 if (wafToken != null) {
 // token available
 } else {
 // error occurred in token refresh
```

```
 }
};

// Add this callback to application creation or activity creation where token will
 be used
tokenProvider.onTokenReady(callback);

// Once you have token in token result callback
// if background refresh is enabled you can call getToken() from same tokenprovider
 object
// if background refresh is disabled you can directly call getToken()(blocking call)
 for new token
WAFToken token = tokenProvider.getToken();
```

Exemple en Kotlin :

```
import com.amazonaws.waf.mobilesdk.token.WAFConfiguration
import com.amazonaws.waf.mobilesdk.token.WAFTokenProvider

private lateinit var wafConfiguration: WAFConfiguration
private lateinit var wafTokenProvider: WAFTokenProvider

private val WAF_INTEGRATION_URL = "Web ACL integration URL"
private val WAF_DOMAIN_NAME = "Domain name"

fun initWaf() {
 // Initialize the tokenprovider instance
 val applicationIntegrationURL = URL(WAF_INTEGRATION_URL)
 wafConfiguration =
  WAFConfiguration.builder().applicationIntegrationURL(applicationIntegrationURL)
   .domainName(WAF_DOMAIN_NAME).backgroundRefreshEnabled(true).build()
 wafTokenProvider = WAFTokenProvider(getApplication(), wafConfiguration)

  // getToken from tokenprovider object
  println("WAF: "+ wafTokenProvider.token.value)

  // implement callback for where token will be used
  wafTokenProvider.onTokenReady {
   wafToken, sdkError ->
  run {
   println("WAF Token:" + wafToken.value)
  }
 }
```

```
}
```

Autoriser le SDK à fournir le cookie jeton dans vos requêtes HTTP

Si `setTokenCookie` tel est le cas`TRUE`, le fournisseur de jetons inclut le cookie jeton pour vous dans vos requêtes Web adressées à tous les emplacements situés sous le chemin spécifié dans`tokenCookiePath`. Par défaut, `setTokenCookie` est `TRUE` et `tokenCookiePath` est`/`.

Vous pouvez réduire la portée des demandes qui incluent un cookie jeton en spécifiant le chemin du cookie jeton, par exemple,`/web/login`. Dans ce cas, vérifiez que vos AWS WAF règles ne détectent pas la présence de jetons dans les demandes que vous envoyez à d'autres chemins. Lorsque vous utilisez le groupe de `AWSManagedRulesACFPRuleSet` règles, vous configurez les chemins d'enregistrement et de création du compte, et le groupe de règles vérifie la présence de jetons dans les demandes envoyées à ces chemins. Pour plus d’informations, consultez Ajouter le groupe de règles géré par l'ACFP à votre ACL Web. De même, lorsque vous utilisez le groupe de `AWSManagedRulesATPRuleSet` règles, vous configurez le chemin de connexion, et le groupe de règles vérifie la présence de jetons dans les demandes envoyées vers ce chemin. Pour plus d’informations, consultez Ajouter le groupe de règles géré par ATP à votre ACL Web.

iOS

Dans `setTokenCookie` ce cas`TRUE`, le fournisseur de jetons stocke le AWS WAF jeton dans un `HTTPCookieStorage.shared` et inclut automatiquement le cookie dans les demandes adressées au domaine que vous avez spécifié`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

Dans `setTokenCookie` ce cas`TRUE`, le fournisseur de jetons stocke le AWS WAF jeton dans une `CookieHandler` instance partagée à l'échelle de l'application. Le fournisseur de jetons inclut automatiquement le cookie dans les demandes adressées au domaine que vous avez spécifié`WAFConfiguration`.

Exemple Java :

```
URL url = new URL("Domain name");
```

```
//The token cookie is set automatically as cookie header
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
connection.getResponseCode();
```

Exemple en Kotlin :

```
val url = URL("Domain name")
//The token cookie is set automatically as cookie header
val connection = (url.openConnection() as HttpsURLConnection)
connection.responseCode
```

Si l'instance `CookieHandler` par défaut est déjà initialisée, le fournisseur de jetons l'utilisera pour gérer les cookies. Dans le cas contraire, le fournisseur de jetons initialisera une nouvelle `CookieManager` instance avec le AWS WAF jeton, `CookiePolicy.ACCEPT_ORIGINAL_SERVER` puis définira cette nouvelle instance comme instance par défaut dans`CookieHandler`.

Le code suivant montre comment le SDK initialise le gestionnaire de cookies et le gestionnaire de cookies lorsqu'ils ne sont pas disponibles dans votre application.

Exemple Java :

```
CookieManager cookieManager = (CookieManager) CookieHandler.getDefault();
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = new CookieManager();
 CookieHandler.setDefault(cookieManager);
}
```

Exemple en Kotlin :

```
var cookieManager = CookieHandler.getDefault() as? CookieManager
if (cookieManager == null) {
 // Cookie manager is initialized with CookiePolicy.ACCEPT_ORIGINAL_SERVER
 cookieManager = CookieManager()
 CookieHandler.setDefault(cookieManager)
}
```

Fournir manuellement le cookie jeton dans vos requêtes HTTP

Si vous définissez cette `setTokenCookie` optionFALSE, vous devez fournir le cookie jeton manuellement, sous forme d'en-tête de requête HTTP Cookie, dans vos demandes adressées à votre point de terminaison protégé. Le code suivant montre comment procéder.

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

Exemple Java :

```
URL url = new URL("Domain name");
HttpsURLConnection connection = (HttpsURLConnection) url.openConnection();
String wafTokenCookie = "aws-waf-token=token from token provider";
connection.setRequestProperty("Cookie", wafTokenCookie);
connection.getInputStream();
```

Exemple en Kotlin :

```
val url = URL("Domain name")
val connection = (url.openConnection() as HttpsURLConnection)
val wafTokenCookie = "aws-waf-token=token from token provider"
connection.setRequestProperty("Cookie", wafTokenCookie)
connection.inputStream
```

CAPTCHAet Challenge dans AWS WAF

Vous pouvez configurer vos AWS WAF règles pour exécuter une Challenge action CAPTCHA ou une action contre les requêtes Web qui répondent aux critères d'inspection de votre règle. Vous pouvez également programmer vos applications JavaScript clientes pour exécuter des puzzles CAPTCHA et des défis de navigateur localement.

Les puzzles CAPTCHA et les défis silencieux ne peuvent être exécutés que lorsque les navigateurs accèdent à des points de terminaison HTTPS. Les clients du navigateur doivent fonctionner dans des contextes sécurisés pour acquérir des jetons.

- CAPTCHA— Demande à l'utilisateur final de résoudre un casse-tête CAPTCHA pour prouver qu'un être humain envoie la demande. Les puzzles CAPTCHA sont conçus pour être assez faciles et rapides à compléter avec succès pour les humains et difficiles pour les ordinateurs à les terminer avec succès ou au hasard avec un taux de réussite significatif.

  Dans les règles ACL du Web, le CAPTCHA est couramment utilisé lorsqu'une Block action arrête un trop grand nombre de demandes légitimes, mais que le fait de laisser passer tout le trafic entraîne des niveaux inacceptables de demandes indésirables, provenant par exemple de robots. Pour plus d'informations sur le comportement des actions des règles, consultezComment fonctionnent les actions AWS WAFCAPTCHA et les Challenge règles.

  Vous pouvez également programmer une implémentation de puzzle CAPTCHA dans les API d'intégration de vos applications clientes. Vous pouvez ainsi personnaliser le comportement et le placement du puzzle dans votre application cliente. Pour plus d'informations, consultez AWS WAF intégration d'applications clientes.
- Challenge— Lance un défi silencieux qui demande à la session client de vérifier qu'il s'agit d'un navigateur et non d'un bot. La vérification s'exécute en arrière-plan sans impliquer l'utilisateur final. Il s'agit d'une bonne option pour vérifier les clients que vous soupçonnez d'être invalides sans nuire à l'expérience de l'utilisateur final avec un casse-tête CAPTCHA. Pour plus d'informations sur le comportement des actions des règles, consultezComment fonctionnent les actions AWS WAFCAPTCHA et les Challenge règles.

  L'action de la Challenge règle est similaire au défi lancé par les API d'intégration intelligente des menaces du client, décrit à l'adresseAWS WAF intégration d'applications clientes.

> **Note**
>
> Des frais supplémentaires vous sont facturés lorsque vous utilisez l'action CAPTCHA ou la Challenge règle dans l'une de vos règles ou en tant que dérogation d'action de règle dans un groupe de règles. Pour plus d'informations, consultez Tarification d'AWS WAF.

Pour une description de toutes les options d'action des règles, consultezAction de la règle.

Rubriques

AWS WAF Puzzles CAPTCHA

AWS WAF fournit une fonctionnalité CAPTCHA standard qui met les utilisateurs au défi de confirmer qu'ils sont des êtres humains. CAPTCHA est l'abréviation de Completely Automated Public Turing Test pour différencier les ordinateurs des humains. Les casse-têtes CAPTCHA sont conçus pour vérifier qu'un humain envoie des demandes et pour empêcher des activités telles que le scraping Web, le bourrage d'informations d'identification et le spam. Les puzzles CAPTCHA ne peuvent pas éliminer toutes les demandes indésirables. De nombreuses énigmes ont été résolues grâce à l'apprentissage automatique et à l'intelligence artificielle. Dans le but de contourner le CAPTCHA, certaines organisations complètent les techniques automatisées par une intervention humaine. Malgré cela, le CAPTCHA continue d'être un outil utile pour empêcher le trafic de bots moins sophistiqué et pour augmenter les ressources requises pour les opérations à grande échelle.

AWS WAF génère aléatoirement ses puzzles CAPTCHA et les fait pivoter pour s'assurer que les utilisateurs sont confrontés à des défis uniques. AWS WAF ajoute régulièrement de nouveaux types et styles de puzzles pour rester efficace contre les techniques d'automatisation. Outre les énigmes, le script AWS WAF CAPTCHA collecte des données sur le client pour s'assurer que la tâche est exécutée par un humain et pour empêcher les attaques en replay.

Chaque casse-tête CAPTCHA comprend un ensemble standard de commandes permettant à l'utilisateur final de demander un nouveau puzzle, de passer d'un puzzle audio à un puzzle visuel, d'accéder à des instructions supplémentaires et de soumettre une solution de puzzle. Tous les puzzles incluent la prise en charge des lecteurs d'écran, des commandes du clavier et des couleurs contrastées.

Les puzzles AWS WAF CAPTCHA répondent aux exigences des Règles pour l'accessibilité des contenus Web (WCAG). Pour plus d'informations, consultez la présentation des règles pour l'accessibilité des contenus Web (WCAG) sur le site Web du World Wide Web Consortium (W3C).

Rubriques

Support du langage de puzzle CAPTCHA

Le casse-tête CAPTCHA commence par des instructions écrites dans la langue du navigateur client ou, si la langue du navigateur n'est pas prise en charge, en anglais. Le puzzle propose des options de langue alternatives via un menu déroulant.

L'utilisateur peut passer aux instructions audio en sélectionnant l'icône du casque au bas de la page. La version audio du puzzle fournit des instructions vocales sur le texte que l'utilisateur doit taper dans une zone de texte, recouvert d'un bruit de fond.

Le tableau suivant répertorie les langues que vous pouvez sélectionner pour les instructions écrites d'un casse-tête CAPTCHA et le support audio pour chaque sélection.

AWS WAF Langues prises en charge par les puzzles CAPTCHA

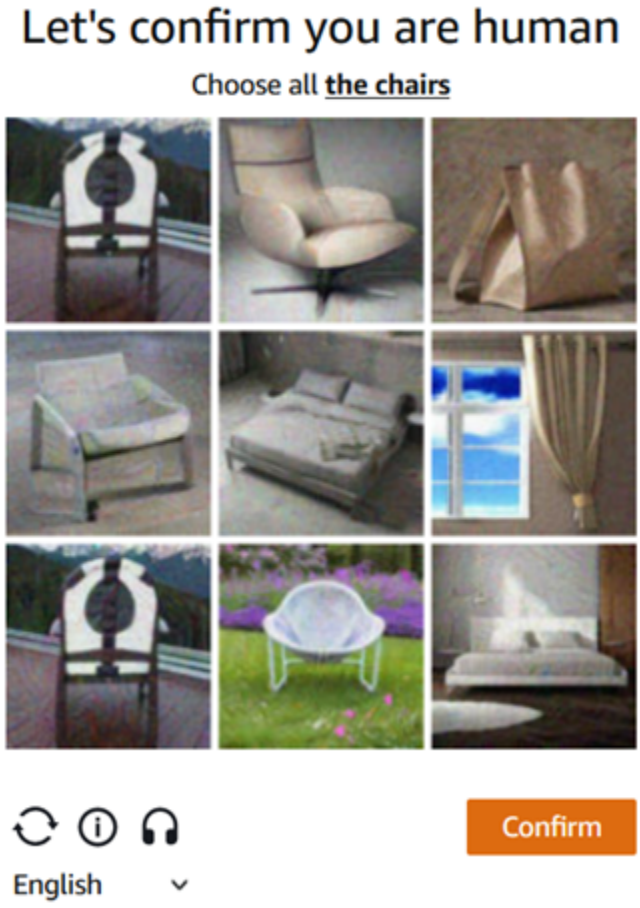
Support des instructions écrites	Code local	Support des instructions audio
Arabe	Ar-sa	Arabe
Chinois (simplifié)	zh-CN	Audio en anglais
Néerlandais	nl-NL	Néerlandais
Anglais	en-US	Anglais
Français	fr-FR	Français
Allemand	de-DE	Allemand
Italien	it-IT	Italien
Japonais	ja-JP	Audio en anglais
Portugais brésilien	pt-BR	Portugais brésilien

Support des instructions écrites	Code local	Support des instructions audio
Espagnol	es-ES	Espagnol
Turc	tr-TR	Turc

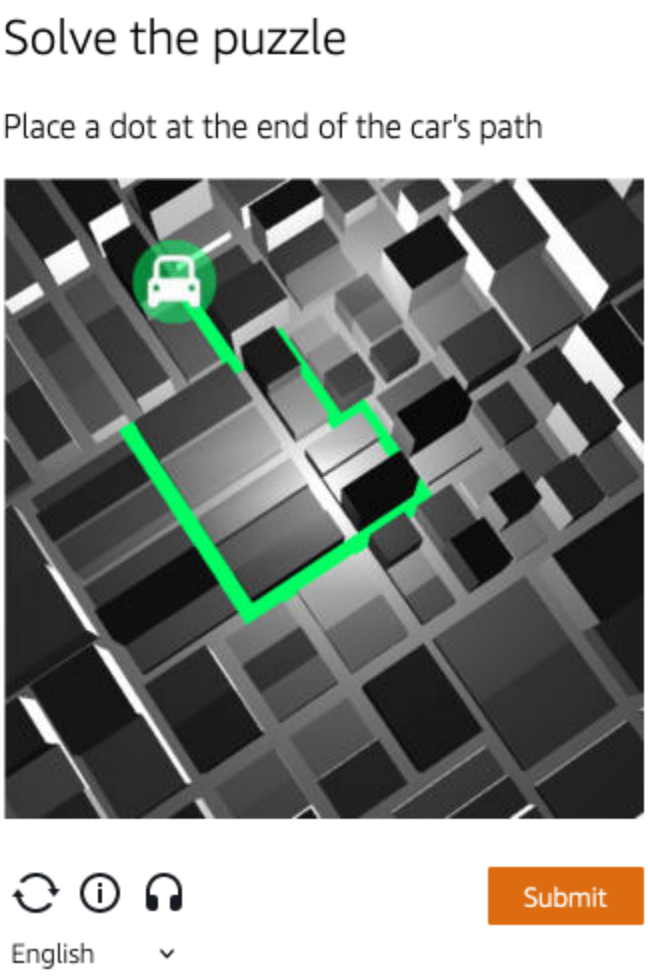
Exemples de casse-têtes CAPTCHA

Un casse-tête CAPTCHA visuel typique nécessite une interaction pour montrer que l'utilisateur peut comprendre et interagir avec une ou plusieurs images.

La capture d'écran suivante montre un exemple de puzzle en grille d'images. Ce casse-tête vous oblige à sélectionner toutes les images de la grille qui incluent un type d'objet spécifique.

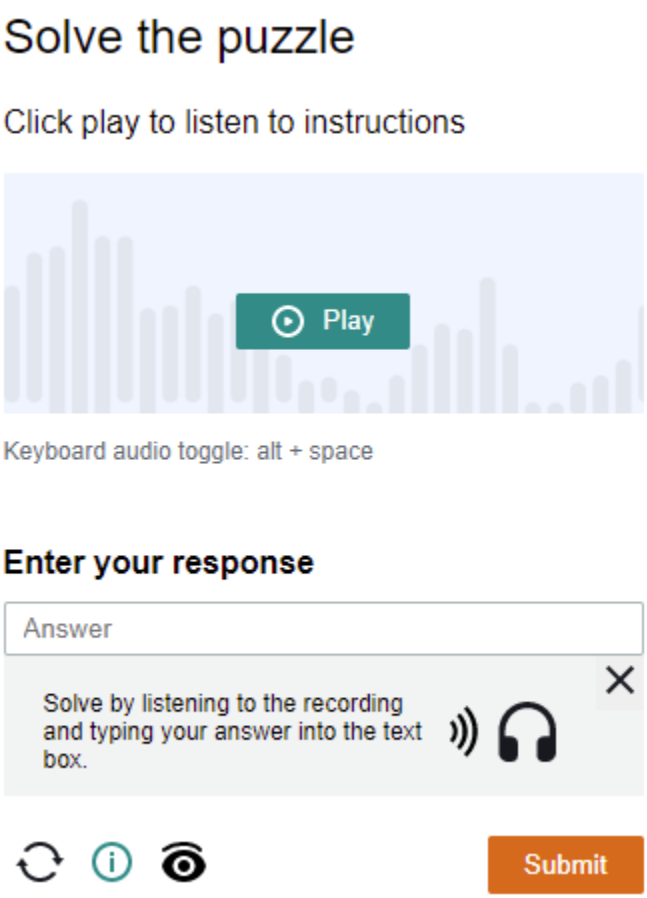


La capture d'écran suivante montre un exemple de puzzle dans lequel vous devez identifier le point final de la trajectoire d'une voiture sur un dessin.



Un puzzle audio produit un bruit de fond recouvert d'instructions vocales concernant le texte que l'utilisateur doit taper dans une zone de texte.

La capture d'écran suivante montre l'affichage du choix du puzzle audio.



Comment fonctionnent les actions AWS WAFCAPTCHA et les Challenge règles

AWS WAF CAPTCHAet Challenge sont des actions de règles standard, elles sont donc relativement faciles à mettre en œuvre. Pour utiliser l'un ou l'autre, vous devez créer les critères d'inspection de votre règle qui identifient les demandes que vous souhaitez inspecter, puis vous spécifiez l'une des deux actions de règle. Pour des informations générales sur les options d'action des règles, consultezAction de la règle.

En plus de mettre en œuvre des défis silencieux et des puzzles CAPTCHA côté serveur, vous pouvez intégrer des défis silencieux dans vos applications clientes JavaScript iOS et Android, et vous pouvez créer des puzzles CAPTCHA chez vos clients. JavaScript Ces intégrations vous permettent de fournir à vos utilisateurs finaux de meilleures performances et de meilleures expériences en matière de casse-tête CAPTCHA, et elles peuvent réduire les coûts associés à l'utilisation des actions de règles et des groupes de règles d'atténuation intelligente des menaces. Pour plus d’informations sur ces options, consultez AWS WAF intégration d'applications clientes. Pour de plus amples informations sur la tarification, veuillez consulter AWS WAF Pricing (français non garanti).

Rubriques

CAPTCHAet comportement Challenge d'action

Lorsqu'une requête Web correspond aux critères d'inspection d'une règle CAPTCHA ou d'une Challenge action, AWS WAF détermine comment traiter la demande en fonction de l'état de son jeton et de la configuration du temps d'immunité. AWS WAF détermine également si la demande peut gérer le casse-tête CAPTCHA ou les interstitiels du script de défi. Les scripts sont conçus pour être traités comme du contenu HTML, et ils ne peuvent être gérés correctement que par un client qui attend du contenu HTML.

> **Note**
>
> Des frais supplémentaires vous sont facturés lorsque vous utilisez l'action CAPTCHA ou la Challenge règle dans l'une de vos règles ou en tant que dérogation d'action de règle dans un groupe de règles. Pour plus d'informations, consultez Tarification d'AWS WAF.

Comment l'action gère la requête Web

AWS WAF applique l'Challengeaction CAPTCHA ou à une requête Web comme suit :

- Jeton valide : AWS WAF gère cela de la même manière qu'une Count action. AWS WAF applique toutes les étiquettes et personnalisations de demande que vous avez configurées pour l'action de règle, puis continue d'évaluer la demande en utilisant les autres règles de l'ACL Web.
- Jeton manquant, non valide ou expiré : AWS WAF interrompt l'évaluation ACL Web de la demande et l'empêche d'atteindre sa destination prévue.

  AWS WAF génère une réponse qu'il renvoie au client, selon le type d'action de la règle :

  - Challenge— AWS WAF inclut les éléments suivants dans la réponse :
    - L'en-tête `x-amzn-waf-action` avec une valeur de `challenge`.

> **Note**
>
> Cet en-tête n'est pas disponible pour JavaScript les applications qui s'exécutent dans le navigateur client. Pour plus de détails, consultez la section qui suit.

- Le code d'état HTTP `202 Request Accepted`.
- Si la demande contient un `Accept` en-tête dont la valeur est égale à`text/html`, la réponse inclut une JavaScript page interstitielle contenant un script de défi.

- CAPTCHA— AWS WAF inclut les éléments suivants dans la réponse :
  - L'en-tête `x-amzn-waf-action` avec une valeur de `captcha`.

> **Note**
>
> Cet en-tête n'est pas disponible pour JavaScript les applications qui s'exécutent dans le navigateur client. Pour plus de détails, consultez la section qui suit.

  - Le code d'état HTTP `405 Method Not Allowed`.
  - Si la demande contient un `Accept` en-tête dont la valeur est égale à`text/html`, la réponse inclut une JavaScript page interstitielle contenant un script CAPTCHA.

Pour configurer le délai d'expiration des jetons au niveau de l'ACL Web ou de la règle, consultezExpiration de l'horodatage : durée d'immunité des AWS WAF jetons.

Les en-têtes ne sont pas disponibles pour JavaScript les applications qui s'exécutent dans le navigateur client

Lorsqu'il AWS WAF répond à une demande client par un CAPTCHA ou une réponse à un défi, il n'inclut pas les en-têtes de partage de ressources entre origines (CORS). Les en-têtes CORS sont un ensemble d'en-têtes de contrôle d'accès qui indiquent au navigateur Web du client quels domaines, méthodes HTTP et en-têtes HTTP peuvent être utilisés par les applications. JavaScript Sans en-têtes CORS, les JavaScript applications exécutées dans un navigateur client n'ont pas accès aux en-têtes HTTP et ne peuvent donc pas lire l'`x-amzn-waf-action`en-tête fourni dans les CAPTCHA réponses et. Challenge

À quoi servent le challenge et les interstitiels CAPTCHA

Lorsqu'un défi interstitiel s'exécute, une fois que le client a répondu avec succès, s'il n'a pas encore de jeton, l'interstitiel en initialise un pour celui-ci. Ensuite, il met à jour le jeton avec l'horodatage de résolution du défi.

Lorsqu'un interstitiel CAPTCHA s'exécute, si le client n'a pas encore de jeton, l'interstitiel CAPTCHA invoque d'abord le script de défi pour défier le navigateur et initialiser le jeton. Ensuite, l'interstitiel exécute son casse-tête CAPTCHA. Lorsque l'utilisateur final termine le puzzle avec succès, l'interstitiel met à jour le jeton avec l'horodatage de résolution du CAPTCHA.

Dans les deux cas, une fois que le client a répondu avec succès et que le script a mis à jour le jeton, le script soumet à nouveau la demande Web d'origine à l'aide du jeton mis à jour.

Vous pouvez configurer le mode de AWS WAF gestion des jetons. Pour plus d'informations, consultez AWS WAF jetons de demande Web.

CAPTCHAet Challenge actions dans les journaux et les métriques

Les Challenge actions CAPTCHA et peuvent être non terminales, similaires, ou terminalesCount, comme. Block Le résultat dépend de la validité ou non d'un jeton valide de la demande avec un horodatage non expiré pour le type d'action.

- Jeton valide : lorsque l'action trouve un jeton valide et ne bloque pas la demande, AWS WAF capture les métriques et les journaux comme suit :
  - Incrémente les métriques pour `RequestsWithValidCaptchaToken` ou `CaptchaRequests` pour `ChallengeRequests` et`RequestsWithValidChallengeToken`.
  - Enregistre la correspondance sous forme d'`nonTerminatingMatchingRules`entrée avec l'action de CAPTCHA ouChallenge. La liste suivante montre la section d'un journal pour ce type de correspondance avec l'CAPTCHAaction.

```
    "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
      }
    }
  ]
```

- Jeton manquant, non valide ou expiré : lorsque l'action bloque la demande en raison d'un jeton manquant ou non valide, AWS WAF capture les métriques et les journaux comme suit :
  - Incrémente la métrique pour `CaptchaRequests` ou`ChallengeRequests`.
  - Enregistre la correspondance en tant qu'`CaptchaResponse`entrée avec un code d'`405`état HTTP ou en tant qu'`ChallengeResponse`entrée avec un code d'`202`état HTTP. Le journal indique s'il manquait le jeton ou si l'horodatage de la demande avait expiré. Le journal indique également s'il s' AWS WAF agit d'une page interstitielle CAPTCHA envoyée au client ou d'un défi silencieux au navigateur du client. La liste suivante indique les sections d'un journal relatives à ce type de correspondance avec l'CAPTCHAaction.

```
"terminatingRuleId": "captcha-rule",
"terminatingRuleType": "REGULAR",
"action": "CAPTCHA",
"terminatingRuleMatchDetails": [],
...
"responseCodeSent": 405,
...
"captchaResponse": {
  "responseCode": 405,
  "solveTimestamp": 0,
  "failureReason": "TOKEN_MISSING"
}
```

Pour plus d'informations sur les AWS WAF journaux, consultezJournalisation AWS WAF du trafic ACL Web.

Pour plus d'informations sur AWS WAF les métriques, consultezAWS WAF métriques et dimensions.

Pour plus d'informations sur les options d'action des règles, consultezAction de la règle.

Bonnes pratiques d'utilisation des Challenge actions CAPTCHA et

Suivez les instructions de cette section pour planifier et mettre en œuvre le AWS WAF CAPTCHA ou le challenge.

Planifiez votre CAPTCHA et testez la mise en œuvre

Déterminez où placer les puzzles CAPTCHA ou les défis silencieux en fonction de l'utilisation de votre site Web, de la sensibilité des données que vous souhaitez protéger et du type de demandes. Sélectionnez les requêtes pour lesquelles vous allez appliquer le CAPTCHA afin de présenter les

puzzles selon les besoins, mais évitez de les présenter là où ils ne seraient pas utiles et pourraient dégrader l'expérience utilisateur. Utilisez cette Challenge action pour exécuter des défis silencieux qui ont moins d'impact sur l'utilisateur final, tout en permettant de vérifier que la demande provient d'un navigateur JavaScript activé.

Les puzzles CAPTCHA et les défis silencieux ne peuvent être exécutés que lorsque les navigateurs accèdent à des points de terminaison HTTPS. Les clients du navigateur doivent fonctionner dans des contextes sécurisés pour acquérir des jetons.

Décidez où lancer les puzzles CAPTCHA et les défis silencieux à vos clients

Identifiez les demandes que vous ne souhaitez pas voir affectées par le CAPTCHA, par exemple les demandes de CSS ou d'images. Utilisez le CAPTCHA uniquement lorsque cela est nécessaire. Par exemple, si vous prévoyez d'effectuer une vérification CAPTCHA lors de la connexion et que l'utilisateur passe toujours directement de l'identifiant à un autre écran, il ne sera probablement pas nécessaire d'exiger une vérification CAPTCHA sur le deuxième écran et cela pourrait dégrader votre expérience utilisateur final.

Configurez Challenge et CAPTCHA utilisez-le de manière à ce AWS WAF qu'il n'envoie que des puzzles CAPTCHA et des défis silencieux en réponse à `GET text/html` des demandes. Vous ne pouvez exécuter ni le puzzle ni le défi en réponse à des `POST` demandes, à des demandes de partage de ressources entre origines (CORS) avant le vol ou à tout autre type de `OPTIONS` demande autre que le type de demande. `GET` Le comportement du navigateur pour les autres types de requêtes peut varier et peut ne pas être en mesure de gérer correctement les interstitiels.

Il est possible qu'un client accepte le HTML mais ne soit toujours pas en mesure de gérer le CAPTCHA ou de défier l'interstitiel. Par exemple, un widget sur une page Web avec un petit iFrame peut accepter le HTML mais ne pas être en mesure d'afficher un CAPTCHA ou de le traiter. Évitez de placer les actions de règle pour ces types de demandes, de la même manière que pour les demandes qui n'acceptent pas le HTML.

Utiliser CAPTCHA ou Challenge vérifier l'acquisition antérieure de jetons

Vous pouvez utiliser les actions des règles uniquement pour vérifier l'existence d'un jeton valide, aux endroits où les utilisateurs légitimes doivent toujours en avoir un. Dans ces situations, peu importe que la demande puisse gérer les interstitiels.

Par exemple, si vous implémentez l'API CAPTCHA de l'application JavaScript client et que vous exécutez le puzzle CAPTCHA sur le client juste avant d'envoyer la première demande à votre point

de terminaison protégé, votre première demande doit toujours inclure un jeton valide à la fois pour le challenge et pour le CAPTCHA. Pour plus d'informations sur l'intégration des applications JavaScript clientes, consultezAWS WAF JavaScript intégrations.

Dans ce cas, dans votre ACL Web, vous pouvez ajouter une règle correspondant à ce premier appel et la configurer avec l'action de CAPTCHA règle Challenge or. Lorsque la règle correspond à un utilisateur final et à un navigateur légitimes, l'action trouvera un jeton valide et ne bloquera donc pas la demande ni n'enverra de défi ou de casse-tête CAPTCHA en réponse. Pour plus d'informations sur le fonctionnement des actions des règles, consultezCAPTCHAet comportement Challenge d'action.

Protégez vos données sensibles non HTML avec et CAPTCHAChallenge

Vous pouvez utiliser le CAPTCHA et Challenge les protections pour les données sensibles non HTML, telles que les API, en suivant l'approche suivante.

1. Identifiez les demandes qui acceptent des réponses HTML et qui sont exécutées à proximité des demandes concernant vos données sensibles non HTML.
2. CAPTCHARédigez des Challenge règles qui correspondent aux demandes de code HTML et aux demandes relatives à vos données sensibles.
3. Ajustez vos paramètres de durée CAPTCHA et d'Challengeimmunité afin que, pour les interactions normales avec les utilisateurs, les jetons que les clients obtiennent à partir des requêtes HTML soient disponibles et non expirés dans leurs demandes concernant vos données sensibles. Pour plus d'informations sur le réglage, voirExpiration de l'horodatage : durée d'immunité des AWS WAF jetons.

Lorsqu'une demande concernant vos données sensibles correspond à une Challenge règle CAPTCHA OR, elle ne sera pas bloquée si le client possède toujours un jeton valide issu du puzzle ou du défi précédent. Si le jeton n'est pas disponible ou si l'horodatage est expiré, la demande d'accès à vos données sensibles échouera. Pour plus d'informations sur le fonctionnement des actions des règles, consultezCAPTCHAet comportement Challenge d'action.

Utilisez le CAPTCHA Challenge pour ajuster vos règles existantes

Passez en revue vos règles existantes pour voir si vous souhaitez les modifier ou les compléter. Voici quelques scénarios courants à envisager.

- Si vous avez une règle basée sur le taux qui bloque le trafic, mais que vous maintenez la limite de débit relativement élevée pour éviter de bloquer les utilisateurs légitimes, envisagez d'ajouter une

deuxième règle basée sur le taux après la règle de blocage. Donnez à la deuxième règle une limite inférieure à la règle de blocage et définissez l'action de la règle sur CAPTCHA ouChallenge. La règle de blocage bloquera toujours les demandes qui arrivent à un rythme trop élevé, et la nouvelle règle bloquera la plupart du trafic automatisé à un taux encore plus faible. Pour plus d'informations sur les règles basées sur les taux, consultezInstruction de règle basée sur un taux.

- Si vous avez un groupe de règles géré qui bloque les demandes, vous pouvez modifier le comportement de certaines ou de toutes les règles de CAPTCHA ou Block versChallenge. Pour ce faire, dans la configuration du groupe de règles géré, remplacez le paramètre d'action de la règle. Pour plus d'informations sur le remplacement des actions des règles, consultezLes actions des règles du groupe de règles remplacent les actions.

Testez votre CAPTCHA et testez les implémentations avant de les déployer

Pour toutes les nouvelles fonctionnalités, suivez les instructions surthe section called “Tester et ajuster vos protections”.

Pendant les tests, passez en revue les exigences d'expiration de l'horodatage de vos jetons et définissez les configurations de votre ACL Web et de la durée d'immunité au niveau des règles afin de trouver un bon équilibre entre le contrôle de l'accès à votre site Web et l'offre d'une bonne expérience à vos clients. Pour plus d’informations, veuillez consulter Expiration de l'horodatage : durée d'immunité des AWS WAF jetons.

Journalisation AWS WAF du trafic ACL Web

Vous pouvez activer la journalisation pour obtenir des informations détaillées sur le trafic qui est analysé par votre liste ACL web. Les informations enregistrées incluent l'heure à laquelle une demande Web AWS WAF a été reçue de votre AWS ressource, des informations détaillées sur la demande et des détails sur les règles auxquelles la demande correspondait. Vous pouvez envoyer des journaux ACL Web à un groupe de CloudWatch journaux Amazon Logs, à un bucket Amazon Simple Storage Service (Amazon S3) ou à un flux de diffusion Amazon Data Firehose.

Autres options de collecte et d'analyse des données

Outre la journalisation, vous pouvez activer les options suivantes pour la collecte et l'analyse des données :

- Amazon Security Lake : vous pouvez configurer Security Lake pour collecter des données ACL Web. Security Lake collecte les données des journaux et des événements à partir de diverses

sources à des fins de normalisation, d'analyse et de gestion. Pour plus d'informations sur cette option, consultez Qu'est-ce qu'Amazon Security Lake ? et Collecte de données à partir AWS des services décrits dans le guide de l'utilisateur d'Amazon Security Lake.

AWS WAF l'utilisation de cette option ne vous est pas facturée. Pour plus d'informations sur les tarifs, consultez les sections Tarification de Security Lake et Comment la tarification de Security Lake est déterminée dans le guide de l'utilisateur d'Amazon Security Lake.

- Échantillonnage de demandes — Vous pouvez configurer votre ACL Web pour échantillonner les requêtes Web qu'elle évalue, afin d'avoir une idée du type de trafic que votre application reçoit. Pour de plus amples informations sur cette option, veuillez consulter Affichage d'un exemple de demandes web.

> **Note**
>
> La configuration de journalisation Web ACL affecte uniquement les AWS WAF journaux. En particulier, la configuration des champs expurgés pour la journalisation n'a aucun impact sur l'échantillonnage des demandes ou sur la collecte de données par Security Lake. La collecte de données Security Lake est entièrement configurée via le service Security Lake. La seule façon d'exclure des champs des demandes échantillonnées est de désactiver l'échantillonnage pour l'ACL Web.

Rubriques

Tarification de l'enregistrement des informations relatives au trafic ACL Web

La journalisation des informations de trafic ACL Web vous est facturée en fonction des coûts associés à chaque type de destination de journal. Ces frais s'ajoutent aux frais d'utilisation AWS WAF. Vos coûts peuvent varier en fonction de facteurs tels que le type de destination que vous choisissez et la quantité de données que vous enregistrez.

Vous trouverez ci-dessous des liens vers les informations tarifaires pour chaque type de destination de journalisation :

- CloudWatch Journaux — Les frais concernent la livraison de bûches par voie automatique. Consultez les tarifs d'Amazon CloudWatch Logs. Sous Paid Tier, choisissez l'onglet Logs, puis sous Vended Logs, consultez les informations relatives à la livraison aux CloudWatch journaux.
- Compartiments Amazon S3 — Les frais Amazon S3 sont les frais combinés pour la livraison CloudWatch des journaux vers les compartiments Amazon S3 et pour l'utilisation d'Amazon S3.
  - Pour Amazon S3, consultez la tarification d'Amazon S3.
  - Pour la livraison CloudWatch des journaux par Logs à Amazon S3, consultez la tarification d'Amazon CloudWatch Logs. Sous Paid Tier, choisissez l'onglet Logs, puis sous Vended Logs, consultez les informations relatives à la livraison à S3
- Firehose — Consultez les tarifs d'Amazon Data Firehose.

Pour plus d'informations sur la AWS WAF tarification, consultez la section AWS WAF Tarification.

AWS WAF destinations de journalisation

Cette section décrit les options de journalisation que vous pouvez choisir pour vos AWS WAF journaux. Chaque section fournit des conseils pour configurer la journalisation, y compris des informations sur tout comportement spécifique au type de destination. Après avoir configuré la destination de journalisation, vous pouvez fournir ses spécifications à la configuration de journalisation de votre ACL Web pour commencer à vous y connecter.

Rubriques

- Groupe de CloudWatch journaux Amazon Logs
- Compartiment Amazon Simple Storage Service
- Flux de livraison d'Amazon Data Firehose

Groupe de CloudWatch journaux Amazon Logs

Cette rubrique fournit des informations sur l'envoi de vos journaux de trafic ACL Web à un groupe de CloudWatch journaux de journaux.

> **Note**
>
> La connexion vous est facturée en plus des frais d'utilisation AWS WAF. Pour plus d'informations, veuillez consulter Tarification de l'enregistrement des informations relatives au trafic ACL Web.

Pour envoyer des journaux à Amazon CloudWatch Logs, vous devez créer un groupe de CloudWatch journaux de journaux. Lorsque vous activez la connexion AWS WAF, vous fournissez l'ARN du groupe de journaux. Une fois que vous avez activé la journalisation pour votre ACL Web, AWS WAF les journaux sont transmis au groupe de CloudWatch journaux Logs sous forme de flux de journaux.

Lorsque vous utilisez CloudWatch Logs, vous pouvez explorer les journaux de votre ACL Web dans la AWS WAF console. Sur votre page ACL Web, sélectionnez l'onglet Logging insights. Cette option s'ajoute aux informations de journalisation fournies aux CloudWatch journaux via la CloudWatch console.

Configurez le groupe de journaux pour les journaux ACL AWS WAF Web dans la même région que l'ACL Web et en utilisant le même compte que celui que vous utilisez pour gérer l'ACL Web. Pour plus d'informations sur la configuration d'un groupe de CloudWatch journaux, consultez la section Utilisation des groupes de journaux et des flux de journaux.

Quotas pour CloudWatch les groupes de journaux

CloudWatch Les journaux ont un quota de débit maximal par défaut, partagé entre tous les groupes de journaux d'une région, que vous pouvez demander à augmenter. Si vos exigences de journalisation sont trop élevées par rapport au paramètre de débit actuel, des mesures de limitation s'afficheront `PutLogEvents` pour votre compte. Pour consulter la limite dans la console Service Quotas et demander une augmentation, consultez le PutLogEvents quota de CloudWatch logs.

Désignation des groupes de journaux

Les noms de vos groupes de journaux doivent commencer par `aws-waf-logs-` et peuvent se terminer par le suffixe de votre choix, `aws-waf-logs-testLogGroup2` par exemple.

Le format ARN obtenu est le suivant :

```
arn:aws:logs:Region:account-id:log-group:aws-waf-logs-log-group-suffix
```

Les flux de journaux ont le format de dénomination suivant :

```
Region_web-acl-name_log-stream-number
```

Voici un exemple de flux de journal pour l'ACL Web `TestWebACL` dans Region`us-east-1`.

```
us-east-1_TestWebACL_0
```

Autorisations requises pour publier des journaux dans CloudWatch Logs

La configuration de la journalisation du trafic Web ACL pour un groupe de CloudWatch journaux de journaux nécessite les paramètres d'autorisation décrits dans cette section. Les autorisations sont définies pour vous lorsque vous utilisez l'une des politiques gérées d'accès AWS WAF complet, `AWSWAFConsoleFullAccess` ou`AWSWAFFullAccess`. Si vous souhaitez gérer un accès plus précis à votre journalisation et à vos AWS WAF ressources, vous pouvez définir vous-même les autorisations. Pour plus d'informations sur la gestion des autorisations, consultez la section Gestion de l'accès aux AWS ressources dans le Guide de l'utilisateur IAM. Pour plus d'informations sur les politiques AWS WAF gérées, consultezAWS politiques gérées pour AWS WAF.

Ces autorisations vous permettent de modifier la configuration de journalisation de l'ACL Web, de configurer la livraison des CloudWatch journaux et de récupérer des informations sur votre groupe de journaux. Ces autorisations doivent être associées à l'utilisateur que vous utilisez pour gérer AWS WAF.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[

            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      }
      {
         "Sid":"WebACLLoggingCWL",
         "Action":[
            "logs:CreateLogDelivery",
```

```
            "logs:DeleteLogDelivery",
            "logs:PutResourcePolicy",
            "logs:DescribeResourcePolicies",
            "logs:DescribeLogGroups"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow"
      }
   ]
}
```

Lorsque des actions sont autorisées sur toutes les AWS ressources, cela est indiqué dans la politique avec un `"Resource"` paramètre de`"*"`. Cela signifie que les actions sont autorisées sur toutes les AWS ressources prises en charge par chaque action. Par exemple, l'action n'`wafv2:PutLoggingConfiguration`est prise en charge que pour la `wafv2` journalisation des ressources de configuration.

Compartiment Amazon Simple Storage Service

Cette rubrique fournit des informations sur l'envoi de vos journaux de trafic ACL Web vers un compartiment Amazon S3.

> **Note**
>
> La connexion vous est facturée en plus des frais d'utilisation AWS WAF. Pour plus d'informations, veuillez consulter Tarification de l'enregistrement des informations relatives au trafic ACL Web.

Pour envoyer vos journaux de trafic ACL Web à Amazon S3, vous configurez un compartiment Amazon S3 à partir du même compte que celui que vous utilisez pour gérer l'ACL Web, et vous nommez le compartiment en commençant par`aws-waf-logs-`. Lorsque vous activez la connexion AWS WAF, vous indiquez le nom du compartiment. Pour plus d'informations sur la création d'un bucket de journalisation, consultez Create a Bucket dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Vous pouvez accéder à vos journaux Amazon S3 et les analyser à l'aide du service de requêtes interactif Amazon Athena. Athena facilite l'analyse des données directement dans Amazon S3 à

l'aide du SQL standard. En effectuant quelques actions AWS Management Console, vous pouvez pointer Athena vers vos données stockées dans Amazon S3 et commencer rapidement à utiliser le SQL standard pour exécuter des requêtes ad hoc et obtenir des résultats. Pour plus d'informations, consultez la section Interrogation des AWS WAF journaux dans le guide de l'utilisateur d'Amazon Athena. Pour des exemples de requêtes Amazon Athena supplémentaires, consultez waf-log-sample-athenaaws-samples/ -queries sur le site Web. GitHub

> **Note**
>
> AWS WAF prend en charge le chiffrement avec des compartiments Amazon S3 pour le type de clé Amazon S3 (SSE-S3) et pour AWS Key Management Service (SSE-KMS). AWS KMS keys AWS WAF ne prend pas en charge le chiffrement des AWS Key Management Service clés gérées par AWS.

Vos ACL Web publient leurs fichiers journaux dans le compartiment Amazon S3 à intervalles de 5 minutes. Chaque fichier journal contient les enregistrements du trafic enregistré au cours des 5 minutes précédentes.

La taille maximale d'un fichier journal est de 75 Mo. Si le fichier journal atteint la taille limite de fichier dans un délai de 5 minutes, le journal arrête d'y ajouter des enregistrements, le publie dans le compartiment Amazon S3, puis crée un nouveau fichier journal.

Les fichiers journaux sont compressés. Si vous ouvrez les fichiers à l'aide de la console Amazon S3, Amazon S3 décompresse les enregistrements du journal et les affiche. Si vous téléchargez les fichiers journaux, vous devez les décompresser pour afficher les enregistrements.

Un seul fichier journal contient des entrées entrelacées avec plusieurs enregistrements. Pour voir tous les fichiers journaux d'une ACL Web, recherchez les entrées agrégées par le nom de l'ACL Web, la région et l'ID de votre compte.

Exigences en matière de dénomination et syntaxe

Les noms de vos compartiments pour la AWS WAF journalisation doivent commencer par `aws-waf-logs-` et peuvent se terminer par le suffixe de votre choix. Par exemple, `aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX`.

Emplacement du godet

Les emplacements des compartiments utilisent la syntaxe suivante :

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/
```

ARN de compartiment

Le format du bucket Amazon Resource Name (ARN) est le suivant :

```
arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX
```

Emplacements des compartiments avec préfixes

Si vous utilisez des préfixes dans le nom de vos clés d'objet pour organiser les données que vous stockez dans vos compartiments, vous pouvez fournir vos préfixes dans les noms de vos compartiments de journalisation.

> **Note**
>
> Cette option n'est pas disponible via la console. Utilisez les AWS WAF API, la CLI ou AWS CloudFormation.

Pour plus d'informations sur l'utilisation des préfixes dans Amazon S3, consultez la section Organisation des objets à l'aide de préfixes dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Les emplacements des compartiments dotés de préfixes utilisent la syntaxe suivante :

```
s3://aws-waf-logs-DOC-EXAMPLE-BUCKET-SUFFIX/DOC-EXAMPLE-KEY-NAME-PREFIX/
```

Dossiers de compartiments et noms de fichiers

À l'intérieur de vos compartiments, et après les préfixes que vous fournissez, vos AWS WAF journaux sont écrits dans une structure de dossiers déterminée par votre identifiant de compte, la région, le nom de l'ACL Web, ainsi que la date et l'heure.

```
AWSLogs/account-id/WAFLogs/Region/web-acl-name/YYYY/MM/dd/HH/mm
```

À l'intérieur des dossiers, les noms des fichiers journaux suivent un format similaire :

```
account-id_waflogs_Region_web-acl-name_timestamp_hash.log.gz
```

Les spécifications temporelles utilisées dans la structure des dossiers et dans le nom du fichier journal sont conformes à la spécification du format d'horodatage. `YYYYMMddTHHmmZ`

Voici un exemple de fichier journal dans un compartiment Amazon S3 pour un compartiment nommé`DOC-EXAMPLE-BUCKET`. L' Compte AWS est`11111111111`. L'ACL Web est `TEST-WEBACL` et la région l'est`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**
>
> Les noms de vos compartiments pour la AWS WAF journalisation doivent commencer par `aws-waf-logs-` et peuvent se terminer par le suffixe de votre choix.

Autorisations requises pour publier des journaux sur Amazon S3

La configuration de la journalisation du trafic ACL Web pour un compartiment Amazon S3 nécessite les paramètres d'autorisation suivants. Ces autorisations sont définies pour vous lorsque vous utilisez l'une des politiques gérées d'accès AWS WAF complet, `AWSWAFConsoleFullAccess` ou`AWSWAFFullAccess`. Si vous souhaitez gérer un accès plus précis à votre journalisation et à vos AWS WAF ressources, vous pouvez définir ces autorisations vous-même. Pour plus d'informations sur la gestion des autorisations, consultez la section Gestion de l'accès aux AWS ressources dans le Guide de l'utilisateur IAM. Pour plus d'informations sur les politiques AWS WAF gérées, consultezAWS politiques gérées pour AWS WAF.

Les autorisations suivantes vous permettent de modifier la configuration de journalisation de l'ACL Web et de configurer la livraison des journaux vers votre compartiment Amazon S3. Ces autorisations doivent être associées à l'utilisateur que vous utilisez pour gérer AWS WAF.

> **Note**
>
> Lorsque vous définissez les autorisations répertoriées ci-dessous, vous pouvez voir des erreurs dans vos AWS CloudTrail journaux indiquant que l'accès a été refusé, mais que les autorisations sont correctes pour la AWS WAF journalisation.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "wafv2:PutLoggingConfiguration",
            "wafv2:DeleteLoggingConfiguration"
         ],
         "Resource":[
            "*"
         ],
         "Effect":"Allow",
         "Sid":"LoggingConfigurationAPI"
      },
    {

       "Sid":"WebACLLogDelivery",

       "Action":[

          "logs:CreateLogDelivery",

          "logs:DeleteLogDelivery"

       ],

       "Resource": "*",

       "Effect":"Allow"

    },
      {
         "Sid":"WebACLLoggingS3",
         "Action":[
            "s3:PutBucketPolicy",
            "s3:GetBucketPolicy"
         ],
         "Resource": [
                "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET"
         ],
         "Effect":"Allow"
      }
   ]
```

```
}
```

Lorsque des actions sont autorisées sur toutes les AWS ressources, cela est indiqué dans la politique avec un `"Resource"` paramètre de`"*"`. Cela signifie que les actions sont autorisées sur toutes les AWS ressources prises en charge par chaque action. Par exemple, l'action n'`wafv2:PutLoggingConfiguration`est prise en charge que pour la `wafv2` journalisation des ressources de configuration.

Par défaut, les compartiments Amazon S3 et les objets qu'ils contiennent sont privés. Seul le propriétaire du compartiment peut accéder au compartiment et aux objets qui y sont stockés. Le propriétaire du bucket peut toutefois accorder l'accès à d'autres ressources et utilisateurs en rédigeant une politique d'accès.

Si l'utilisateur qui crée le journal est propriétaire du compartiment, le service attache automatiquement la politique suivante au compartiment pour autoriser le journal à y publier des journaux :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSLogDeliveryWrite",
      "Effect": "Allow",
      "Principal": {
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/AWSLogs/account-id/*",
      "Condition": {
        "StringEquals": {
          "s3:x-amz-acl": "bucket-owner-full-control",
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    },
    {
      "Sid": "AWSLogDeliveryAclCheck",
      "Effect": "Allow",
      "Principal": {
```

```
        "Service": "delivery.logs.amazonaws.com"
      },
      "Action": "s3:GetBucketAcl",
      "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": ["account-id"]
        },
        "ArnLike": {
          "aws:SourceArn": ["arn:aws:logs:region:account-id:*"]
        }
      }
    }
  ]
}
```

> **Note**
>
> Les noms de vos compartiments pour la AWS WAF journalisation doivent commencer par `aws-waf-logs-` et peuvent se terminer par le suffixe de votre choix.

Si l'utilisateur qui crée le journal n'est pas propriétaire du compartiment ou ne dispose pas des `PutBucketPolicy` autorisations `GetBucketPolicy` et pour le compartiment, la création du journal échoue. Dans ce cas, le propriétaire du compartiment doit ajouter manuellement la politique précédente au compartiment et spécifier l' Compte AWS ID du créateur du journal. Pour de plus amples informations, veuillez consulter Comment ajouter une politique de compartiment S3 dans le Guide de l'utilisateur Amazon Simple Storage Service. Si le bucket reçoit les journaux de plusieurs comptes, ajoutez une entrée d'`Resource`élément à la déclaration de `AWSLogDeliveryWrite` politique pour chaque compte.

Par exemple, la politique de compartiment suivante permet Compte AWS `111122223333` de publier des journaux dans un compartiment nommé `aws-waf-logs-DOC-EXAMPLE-BUCKET` :

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryWrite20150319",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryWrite",
            "Effect": "Allow",
```

```
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
                "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/
AWSLogs/111122223333/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                    "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        },
        {
            "Sid": "AWSLogDeliveryAclCheck",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET",
            "Condition": {
                "StringEquals": {
                "aws:SourceAccount": ["111122223333"]
                },
                "ArnLike": {
                "aws:SourceArn": ["arn:aws:logs:us-east-1:111122223333:*"]
                }
            }
        }
    ]
}
```

Autorisations d'utilisation AWS Key Management Service avec une clé KMS

Si votre destination de journalisation utilise le chiffrement côté serveur avec des clés stockées dans AWS Key Management Service (SSE-KMS) et que vous utilisez une clé gérée par le client (clé KMS), vous devez AWS WAF autoriser l'utilisation de votre clé KMS. Pour ce faire, vous ajoutez une politique clé à la clé KMS pour la destination que vous avez choisie. Cela permet à la AWS WAF journalisation d'écrire vos fichiers journaux vers votre destination.

Ajoutez la politique de clé suivante à votre clé KMS AWS WAF pour autoriser la connexion à votre compartiment Amazon S3.

```
{
    "Sid": "Allow AWS WAF to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": [
            "delivery.logs.amazonaws.com"
        ]
    },
    "Action": "kms:GenerateDataKey*",
    "Resource": "*"
}
```

Autorisations requises pour accéder aux fichiers journaux Amazon S3

Amazon S3 utilise des listes de contrôle d'accès (ACL) pour gérer l'accès aux fichiers journaux créés par un AWS WAF journal. Par défaut, le propriétaire du compartiment dispose d'autorisations `FULL_CONTROL` sur chaque fichier journal. Si le propriétaire de la diffusion des journaux n'est pas le propriétaire du compartiment, il ne dispose d'aucune autorisation. Le compte de diffusion des journaux possède les autorisations `READ` et `WRITE`. Pour de plus amples informations, veuillez consulter Présentation des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Flux de livraison d'Amazon Data Firehose

Cette section fournit des informations sur l'envoi de vos journaux de trafic ACL Web vers un flux de diffusion Amazon Data Firehose.

> **Note**
>
> La connexion vous est facturée en plus des frais d'utilisation AWS WAF. Pour plus d'informations, veuillez consulter Tarification de l'enregistrement des informations relatives au trafic ACL Web.

Pour envoyer des journaux à Amazon Data Firehose, vous devez envoyer des journaux depuis votre ACL Web vers un flux de diffusion Amazon Data Firehose que vous configurez dans Firehose. Après

avoir activé la journalisation, AWS WAF envoie les journaux à votre destination de stockage via le point de terminaison HTTPS de Firehose.

Un AWS WAF journal équivaut à un enregistrement Firehose. Si vous recevez généralement 10 000 requêtes par seconde et que vous activez les journaux complets, vous devriez avoir un paramètre de 10 000 enregistrements par seconde dans Firehose. Si vous ne configurez pas correctement Firehose, tous les journaux ne AWS WAF seront pas enregistrés. Pour plus d'informations, consultez la section Quotas Amazon Kinesis Data Firehose.

Pour savoir comment créer un flux de diffusion Amazon Data Firehose et consulter vos journaux enregistrés, consultez Qu'est-ce qu'Amazon Data Firehose ?

Pour plus d'informations sur la création de votre flux de diffusion, consultez Création d'un flux de diffusion Amazon Data Firehose.

Configuration d'un flux de diffusion Amazon Data Firehose pour votre ACL Web

Configurez un flux de diffusion Amazon Data Firehose pour votre ACL Web comme suit.

- Créez-le en utilisant le même compte que celui que vous utilisez pour gérer l'ACL Web.
- Créez-le dans la même région que l'ACL Web. Si vous capturez des journaux pour Amazon CloudFront, créez le firehose dans la région USA Est (Virginie du Nord),`us-east-1`.
- Donnez au data firehose un nom commençant par le préfixe`aws-waf-logs-`. Par exemple, `aws-waf-logs-us-east-2-analytics`.
- Configurez-le pour le téléchargement direct, ce qui permet aux applications d'accéder directement au flux de diffusion. Dans la console Amazon Data Firehose, pour le paramètre Source du flux de diffusion, choisissez Direct PUT ou autres sources. Par le biais de l'API, définissez la propriété du flux `DeliveryStreamType` de diffusion sur`DirectPut`.

> **Note**
>
> N'utilisez pas a `Kinesis stream` comme source.

Autorisations requises pour publier des journaux dans un flux de diffusion Amazon Data Firehose

Pour comprendre les autorisations requises pour votre configuration Kinesis Data Firehose, consultez la section Contrôle des accès avec Amazon Kinesis Data Firehose.

Vous devez disposer des autorisations suivantes pour activer correctement la journalisation des ACL Web avec un flux de diffusion Amazon Data Firehose.

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Pour plus d'informations sur les rôles liés aux services et les `iam:CreateServiceLinkedRole` autorisations, consultez. Utilisation de rôles liés à un service pour AWS WAF

Configuration de la journalisation des ACL Web

Vous pouvez activer et désactiver la journalisation pour une ACL Web à tout moment.

> **Note**
>
> La connexion vous est facturée en plus des frais d'utilisation AWS WAF. Pour plus d'informations, veuillez consulter Tarification de l'enregistrement des informations relatives au trafic ACL Web.

Si vous ne trouvez aucun enregistrement de journal dans vos journaux

En de rares occasions, il est possible que le taux de livraison des AWS WAF grumes tombe en dessous de 100 %, les journaux étant livrés dans la mesure du possible. L' AWS WAF architecture donne la priorité à la sécurité de vos applications par rapport à toute autre considération. Dans certaines situations, par exemple lorsque les flux de journalisation sont soumis à une limitation du trafic, cela peut entraîner la suppression d'enregistrements. Cela ne devrait pas affecter plus que quelques enregistrements. Si vous remarquez un certain nombre d'entrées de journal manquantes, contactez le AWS Support Centre.

Dans la configuration de journalisation de votre ACL Web, vous pouvez personnaliser ce qui est AWS WAF envoyé aux journaux.

- Rédaction des champs : vous pouvez supprimer les champs suivants des enregistrements du journal pour les règles qui utilisent les paramètres de correspondance correspondants : chemin d'URI, chaîne de requête, en-tête unique et méthode HTTP. Les champs expurgés apparaissent comme `REDACTED` dans les journaux. Par exemple, si vous supprimez le champ Chaîne de

requête, dans les journaux, il sera répertorié comme `REDACTED` pour toutes les règles utilisant le paramètre de correspondance des chaînes de requête. La rédaction s'applique uniquement au composant de demande que vous spécifiez pour la correspondance dans la règle, de sorte que la rédaction du composant d'en-tête unique ne s'applique pas aux règles qui correspondent aux en-têtes. Pour obtenir la liste des champs du journal, consultezChamps de journal.

> **Note**
>
> Ce paramètre n'a aucun impact sur l'échantillonnage des demandes. Avec l'échantillonnage des demandes, le seul moyen d'exclure des champs est de désactiver l'échantillonnage pour l'ACL Web.

- Filtrage des journaux : vous pouvez ajouter un filtrage pour spécifier les requêtes Web qui sont conservées dans les journaux et celles qui sont supprimées. Vous filtrez les paramètres qui AWS WAF s'appliquent lors de l'évaluation de la demande Web. Vous pouvez filtrer selon les paramètres suivants :
  - Étiquette entièrement qualifiée : les étiquettes entièrement qualifiées ont un préfixe, des espaces de noms facultatifs et un nom d'étiquette. Le préfixe identifie le groupe de règles ou le contexte de la liste ACL web de la règle qui a ajouté l'étiquette. Pour plus d'informations sur les étiquettes, consultezAWS WAF étiquettes sur les requêtes Web.
  - Action par règle : vous pouvez filtrer sur n'importe quel paramètre d'action de règle normal ainsi que sur l'ancienne option de `EXCLUDED_AS_COUNT` remplacement pour les règles de groupe de règles. Pour plus d'informations sur les paramètres d'action des règles, consultezAction de la règle. Pour plus d'informations sur les dérogations aux actions des règles actuelles et anciennes pour les règles de groupe de règles, consultezOptions de dérogation aux actions pour les groupes de règles.
    - Les filtres d'action de règle normaux s'appliquent aux actions configurées dans les règles ainsi qu'aux actions configurées à l'aide de l'option actuelle permettant de remplacer une action de règle de groupe de règles.
    - Le filtre du `EXCLUDED_AS_COUNT` journal chevauche le filtre du journal des `Count` actions. `EXCLUDED_AS_COUNT`filtre à la fois les options actuelles et héritées pour remplacer une action de règle de groupe de règles surCount.

Activation de la journalisation pour une ACL Web

Pour activer la journalisation pour une ACL Web, vous devez déjà avoir configuré une destination de journalisation. Pour plus d'informations sur vos choix de destinations et les exigences relatives à chacune d'entre elles, consultezAWS WAF destinations de journalisation.

Pour activer la journalisation pour une liste ACL web

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, choisissez Web ACLs.
3. Choisissez le nom de l'ACL Web pour laquelle vous souhaitez activer la journalisation. La console vous amène à la description de la liste ACL web, où vous pouvez la modifier.
4. Dans l'onglet Journalisation, choisissez Activer la journalisation.
5. Choisissez le type de destination de journalisation, puis choisissez la destination de journalisation que vous avez configurée. Vous devez choisir une destination de journalisation dont le nom commence par`aws-waf-logs-`.
6. (Facultatif) Si vous ne souhaitez pas que certains champs soient inclus dans les journaux, supprimez-les. Choisissez le champ à censurer, puis choisissez Ajouter. Répétez si nécessaire pour censurer des champs supplémentaires.

   > **Note**
   >
   > Ce paramètre n'a aucun impact sur l'échantillonnage des demandes. Avec l'échantillonnage des demandes, le seul moyen d'exclure des champs est de désactiver l'échantillonnage pour l'ACL Web.

7. (Facultatif) Si vous ne souhaitez pas envoyer toutes les demandes aux journaux, ajoutez vos critères de filtrage et votre comportement. Sous Filtrer les journaux, pour chaque filtre que vous souhaitez appliquer, choisissez Ajouter un filtre, puis choisissez vos critères de filtrage et indiquez si vous souhaitez conserver ou supprimer les demandes correspondant à ces critères. Lorsque vous avez fini d'ajouter des filtres, modifiez si nécessaire le comportement de journalisation par défaut.
8. Choisissez Activer la journalisation.

> **Note**
>
> Lorsque vous activez correctement la journalisation, AWS WAF un rôle lié à un service est créé avec les autorisations nécessaires pour écrire des journaux sur la destination de journalisation. Pour plus d'informations, voir Utilisation de rôles liés à un service pour AWS WAF.

Champs de journal

La liste suivante décrit les champs de journal possibles.

action

Action de terminaison AWS WAF appliquée à la demande. Cela indique une autorisation, un blocage, un CAPTCHA ou un défi. Les Challenge actions CAPTCHA et prennent fin lorsque la requête Web ne contient pas de jeton valide.

args

Chaîne de requête.

Réponse au captcha

État de l'action CAPTCHA pour la demande, renseigné lorsqu'une CAPTCHA action est appliquée à la demande. Ce champ est renseigné pour toute CAPTCHA action, qu'elle soit terminale ou non. Si l'CAPTCHAaction est appliquée plusieurs fois à une demande, ce champ est renseigné à partir de la dernière fois que l'action a été appliquée.

L'CAPTCHAaction met fin à l'inspection des demandes Web lorsque la demande n'inclut pas de jeton ou lorsque le jeton n'est pas valide ou a expiré. Si l'CAPTCHAaction prend fin, ce champ inclut un code de réponse et le motif de l'échec. Si l'action n'est pas terminée, ce champ inclut un horodatage de résolution. Pour différencier une action terminante d'une action non terminale, vous pouvez filtrer un `failureReason` attribut non vide dans ce champ.

Réponse au défi

État de l'action de défi pour la demande, renseigné lorsqu'une Challenge action est appliquée à la demande. Ce champ est renseigné pour toute Challenge action, qu'elle soit terminale ou non. Si l'Challengeaction est appliquée plusieurs fois à une demande, ce champ est renseigné à partir de la dernière fois que l'action a été appliquée.

L'Challengeaction met fin à l'inspection des demandes Web lorsque la demande n'inclut pas de jeton ou lorsque le jeton n'est pas valide ou a expiré. Si l'Challengeaction prend fin, ce champ inclut un code de réponse et le motif de l'échec. Si l'action n'est pas terminée, ce champ inclut un horodatage de résolution. Pour différencier une action terminante d'une action non terminale, vous pouvez filtrer un `failureReason` attribut non vide dans ce champ.

clientIp

Adresse IP du client envoyant la requête.

country

Pays source de la requête. S'il n' AWS WAF est pas en mesure de déterminer le pays d'origine, il définit ce champ sur`-`.

excludedRules

Utilisé uniquement pour les règles de groupe de règles. Liste des règles dans le groupe de règles que vous avez exclues. L'action associée à ces règles est définie surCount.

Si vous remplacez une règle pour qu'elle soit prise en compte à l'aide de l'option d'action de remplacement de la règle, les correspondances ne sont pas répertoriées ici. Ils sont répertoriés sous forme de paires d'actions `action` et`overriddenAction`.

exclusionType

Type qui indique que la règle exclue a une actionCount.

ruleId

ID de la règle au sein du groupe de règles qui est exclu.

formatVersion

Version du format du journal.

headers

Liste des en-têtes.

httpMethod

Méthode HTTP de la requête.

httpRequest

Métadonnées relatives à la requête.

httpSourceId

L'ID de la ressource associée :

- Pour une CloudFront distribution Amazon, l'ID est celui indiqué *`distribution-id`* dans la syntaxe de l'ARN :

  `arn:`*`partition`*`cloudfront::`*`account-id`*`:distribution/`*`distribution-id`*

- Pour un Application Load Balancer, l'ID est le suivant *`load-balancer-id`* dans la syntaxe de l'ARN :

  `arn:`*`partition`*`:elasticloadbalancing:`*`region`*`:`*`account-id`*`:loadbalancer/app/`*`load-balancer-name/load-balancer-id`*

- Pour une API REST Amazon API Gateway, l'ID est celui *`api-id`* indiqué dans la syntaxe ARN :

  `arn:`*`partition`*`:apigateway:`*`region`*`::/restapis/`*`api-id`*`/stages/`*`stage-name`*

- Pour une API AWS AppSync GraphQL, l'ID est celui indiqué *`GraphQLApiId`* dans la syntaxe de l'ARN :

  `arn:`*`partition`*`:appsync:`*`region`*`:`*`account-id`*`:apis/`*`GraphQLApiId`*

- Pour un groupe d'utilisateurs Amazon Cognito, l'identifiant est celui indiqué *`user-pool-id`* dans la syntaxe ARN :

  `arn:`*`partition`*`:cognito-idp:`*`region`*`:`*`account-id`*`:userpool/`*`user-pool-id`*

- Pour un AWS App Runner service, l'ID est celui indiqué *`apprunner-service-id`* dans la syntaxe de l'ARN :

  `arn:`*`partition`*`:apprunner:`*`region`*`:`*`account-id`*`:service/`*`apprunner-service-name/apprunner-service-id`*

httpSourceName

Source de la requête. Valeurs possibles : `CF` pour Amazon CloudFront, `APIGW` pour Amazon API Gateway, `ALB` pour Application Load Balancer, `APPSYNC` pour, pour Amazon Cognito AWS AppSync`APPRUNNER`, `COGNITOIDP` pour App Runner `VERIFIED_ACCESS` et pour Verified Access.

httpVersion

Version de HTTP.

Empreinte digitale JA3

L'empreinte JA3 de la demande.

> **Note**
>
> L'inspection des empreintes digitales JA3 n'est disponible que pour les CloudFront distributions Amazon et les équilibreurs de charge d'application.

L'empreinte JA3 est un hachage de 32 caractères dérivé du client TLS Hello d'une demande entrante. Cette empreinte sert d'identifiant unique pour la configuration TLS du client. AWS WAF calcule et enregistre cette empreinte pour chaque demande contenant suffisamment d'informations TLS Client Hello pour le calcul.

Vous fournissez cette valeur lorsque vous configurez une correspondance d'empreinte JA3 dans vos règles ACL Web. Pour plus d'informations sur la création d'une correspondance avec l'empreinte JA3, reportez-vous Empreinte digitale JA3 à l'instruction Options de composants de demande for a rule.

labels

Les étiquettes figurant sur la demande Web. Ces labels ont été appliqués par des règles qui ont été utilisées pour évaluer la demande. AWS WAF enregistre les 100 premières étiquettes.

nonTerminatingMatchingRègles

Liste des règles non résilientes correspondant à la demande. Chaque élément de la liste contient les informations suivantes.

action

Action AWS WAF appliquée à la demande. Cela indique soit le nombre, soit le CAPTCHA, soit le défi. ChallengeLes CAPTCHA et ne se terminent pas lorsque la requête Web contient un jeton valide.

ruleId

L'ID de la règle qui correspondait à la demande et qui ne se terminait pas.

ruleMatchDetails

Informations détaillées sur la règle correspondant à la demande. Ce champ est uniquement renseigné pour les instructions de règles d'injection SQL et de correspondance entre les

scripts intersites (XSS). Une règle de correspondance peut nécessiter une correspondance pour plusieurs critères d'inspection. Ces détails de correspondance sont donc fournis sous la forme d'un tableau de critères de correspondance.

Toute information supplémentaire fournie pour chaque règle varie en fonction de facteurs tels que la configuration de la règle, le type de correspondance des règles et les détails de la correspondance. Par exemple, pour les règles comportant une Challenge action CAPTCHA ou, le `captchaResponse` ou `challengeResponse` sera répertorié. Si la règle correspondante se trouve dans un groupe de règles et que vous avez remplacé son action de règle configurée, l'action configurée sera fournie dans. `overriddenAction`

Champs surdimensionnés

Liste des champs de la requête Web qui ont été inspectés par l'ACL Web et qui dépassent la limite AWS WAF d'inspection. Si un champ est surdimensionné mais que l'ACL Web ne l'inspecte pas, il ne sera pas répertorié ici.

Cette liste peut contenir zéro ou plusieurs des valeurs suivantes : `REQUEST_BODY`REQUEST_JSON_BODY,`REQUEST_HEADERS`, et`REQUEST_COOKIES`. Pour plus d'informations sur les champs surdimensionnés, consultezGestion des composants de demande surdimensionnés dans AWS WAF.

rateBasedRuleListe

Liste de règles basées sur le débit qui ont agi sur la requête. Pour plus d'informations sur les règles basées sur les taux, consultezInstruction de règle basée sur un taux.

rateBasedRuleId

ID de la règle basée sur le débit qui a agi sur la requête. Si cette règle a résilié la requête, l'ID pour `rateBasedRuleId` est le même que pour `terminatingRuleId`.

rateBasedRuleNom

Nom de la règle basée sur le taux qui a donné suite à la demande.

limitKey

Type d'agrégation utilisé par la règle. Les valeurs possibles concernent l'origine de la `IP` demande Web, `FORWARDED_IP` une adresse IP transmise dans un en-tête de la `CUSTOMKEYS` demande, des paramètres clés agrégés personnalisés et `CONSTANT` le comptage de toutes les demandes ensemble, sans agrégation.

Valeur limite

Utilisé uniquement en cas de limitation du débit par un seul type d'adresse IP. Si une demande contient une adresse IP non valide, `limitvalue` c'est`INVALID`.

maxRateAllowed

Le nombre maximum de demandes autorisées dans la fenêtre temporelle spécifiée pour une instance d'agrégation spécifique. L'instance d'agrégation est définie par le `limitKey` plus toute spécification clé supplémentaire que vous avez fournie dans la configuration des règles basées sur le taux.

evaluationWindowSec

Le temps AWS WAF inclus dans sa demande compte, en secondes.

Valeurs personnalisées

Valeurs uniques identifiées par la règle basée sur le taux dans la demande. Pour les valeurs de chaîne, les journaux impriment les 32 premiers caractères de la valeur de chaîne. Selon le type de clé, ces valeurs peuvent être uniquement pour une clé, comme pour la méthode HTTP ou la chaîne de requête, ou pour une clé et un nom, comme pour l'en-tête et le nom de l'en-tête.

requestHeadersInserted

La liste des en-têtes insérés pour le traitement personnalisé des demandes.

requestId

ID de la demande, qui est généré par le service hôte sous-jacent. Pour Application Load Balancer, il s'agit de l'ID de trace. Pour tous les autres, il s'agit de l'ID de demande.

responseCodeSent

Le code de réponse envoyé avec une réponse personnalisée.

ruleGroupId

ID du groupe de règles. Si la règle a bloqué la requête, l'ID pour `ruleGroupID` est le même que pour `terminatingRuleId`.

ruleGroupList

Liste des groupes de règles ayant donné suite à cette demande, avec les informations correspondantes.

terminatingRule

Règle qui a mis fin à la demande. S'il est présent, il contient les informations suivantes.

action

Action de terminaison AWS WAF appliquée à la demande. Cela indique une autorisation, un blocage, un CAPTCHA ou un défi. Les Challenge actions CAPTCHA et prennent fin lorsque la requête Web ne contient pas de jeton valide.

ruleId

ID de la règle correspondant à la demande.

ruleMatchDetails

Informations détaillées sur la règle correspondant à la demande. Ce champ est uniquement renseigné pour les instructions de règles d'injection SQL et de correspondance entre les scripts intersites (XSS). Une règle de correspondance peut nécessiter une correspondance pour plusieurs critères d'inspection. Ces détails de correspondance sont donc fournis sous la forme d'un tableau de critères de correspondance.

Toute information supplémentaire fournie pour chaque règle varie en fonction de facteurs tels que la configuration de la règle, le type de correspondance des règles et les détails de la correspondance. Par exemple, pour les règles comportant une Challenge action CAPTCHA ou, le `captchaResponse` ou `challengeResponse` sera répertorié. Si la règle correspondante se trouve dans un groupe de règles et que vous avez remplacé son action de règle configurée, l'action configurée sera fournie dans. `overriddenAction`

terminatingRuleId

ID de la règle qui a résilié la requête. Si rien ne résilie la requête, la valeur est `Default_Action`.

terminatingRuleMatchDétails

Informations détaillées sur la règle de fin correspondant à la demande. Une règle de fin comporte une action qui met fin au processus d'inspection par rapport à une demande Web. Les actions possibles pour une règle de résiliation incluentAllow, BlockCAPTCHA, etChallenge. Lors de l'inspection d'une requête Web, la première règle correspondant à la demande et comportant une action de fin AWS WAF arrête l'inspection et applique l'action. La requête Web peut contenir d'autres menaces, en plus de celle signalée dans le journal pour la règle de terminaison correspondante.

Cette information n'est renseignée que pour les instructions de règle de correspondance d'injection SQL et de script inter-site (XSS). La règle de correspondance peut nécessiter une correspondance pour plusieurs critères d'inspection. Ces détails de correspondance sont donc fournis sous la forme d'un tableau de critères de correspondance.

terminatingRuleType

Type de règle qui a résilié la requête. Valeurs possibles : RATE_BASED, REGULAR, GROUP et MANAGED_RULE_GROUP.

timestamp

L'horodatage en millisecondes.

uri

URI de la requête.

webaclId

GUID de la liste ACL Web.

Exemples de journaux

Example Règle 1 basée sur le taux : configuration des règles avec une seule clé, définie sur **`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 Règle basée sur le taux 1 : entrée dans le journal pour une demande bloquée par une règle basée sur le taux

```
{
   "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 Règle 2 basée sur le taux : configuration des règles avec deux clés, définies sur et **`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 Règle basée sur le taux 2 : entrée dans le journal pour une demande bloquée par une règle basée sur le taux

```
{
   "timestamp":1633322211194,
   "formatVersion":1,
   "webaclId":...,
   "terminatingRuleId":"RateBasedRule",
   "terminatingRuleType":"RATE_BASED",
   "action":"BLOCK",
   "terminatingRuleMatchDetails":[

   ],
   "httpSourceName":"APIGW",
   "httpSourceId":"EXAMPLE11:rjvegx5guh:CanaryTest",
   "ruleGroupList":[

   ],
   "rateBasedRuleList":[
      {
         "rateBasedRuleId":...,
         "rateBasedRuleName":"RateBasedRule",
         "limitKey":"CUSTOMKEYS",
         "maxRateAllowed":100,
         "evaluationWindowSec":"120",
         "customValues":[
            {
               "key":"HEADER",
```

```
            "name":"dogname",
            "value":"ella"
         },
         {
            "key":"HEADER",
            "name":"catname",
            "value":"goofie"
         }
      ]
   }
],
"nonTerminatingMatchingRules":[

],
"requestHeadersInserted":null,
"responseCodeSent":null,
"httpRequest":{
   "clientIp":"52.46.82.35",
   "country":"FR",
   "headers":[
      {
         "name":"X-Forwarded-For",
         "value":"52.46.82.35"
      },
      {
         "name":"X-Forwarded-Proto",
         "value":"https"
      },
      {
         "name":"X-Forwarded-Port",
         "value":"443"
      },
      {
         "name":"Host",
         "value":"23llbyn8v3.execute-api.eu-west-3.amazonaws.com"
      },
      {
         "name":"X-Amzn-Trace-Id",
         "value":"Root=1-64556629-17ac754c2ed9f0620e0f2a0c"
      },
      {
         "name":"catname",
         "value":"goofie"
      },
```

```
         {
            "name":"dogname",
            "value":"ella"
         },
         {
            "name":"User-Agent",
            "value":"Apache-HttpClient/UNAVAILABLE (Java/11.0.19)"
         },
         {
            "name":"Accept-Encoding",
            "value":"gzip,deflate"
         }
      ],
      "uri":"/CanaryTest",
      "args":"",
      "httpVersion":"HTTP/1.1",
      "httpMethod":"GET",
      "requestId":"EdzmlH5OCGYF1vQ="
   }
}
```

Example Sortie du journal pour une règle déclenchée lors de la détection de SQLi (arrêt)

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:111122223333:regional/webacl/
STMTest/1EXAMPLE-2ARN-3ARN-4ARN-123456EXAMPLE",
    "terminatingRuleId": "STMTest_SQLi_XSS",
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "HIGH",
            "location": "HEADER",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
```

```
    "httpSourceName": "-",
    "httpSourceId": "-",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [
            {
                "name": "Host",
                "value": "localhost:1989"
            },
            {
                "name": "User-Agent",
                "value": "curl/7.61.1"
            },
            {
                "name": "Accept",
                "value": "*/*"
            },
            {
                "name": "x-stm-test",
                "value": "10 AND 1=1"
            }
        ],
        "uri": "/myUri",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "GET",
        "requestId": "rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Sortie du journal pour une règle qui s'est déclenchée lors de la détection de SQLi (sans interruption)

```
{
```

```
    "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 Sortie du journal pour plusieurs règles déclenchées au sein d'un groupe de règles (Rulea-XSS se termine et Rule-B ne se termine pas)

```
{
    "timestamp":1592361810888,
    "formatVersion":1,
    "webaclId":"arn:aws:wafv2:us-east-1:123456789012:global/webacl/hello-
world/5933d6d9-9dde-js82-v8aw-9ck28nv9"
    ,"terminatingRuleId":"RG-Reference"
    ,"terminatingRuleType":"GROUP"
    ,"action":"BLOCK",
    "terminatingRuleMatchDetails":
    [{
        "conditionType":"XSS"
        ,"location":"HEADER"
        ,"matchedData":["<","frameset"]
    }]
    ,"httpSourceName":"-"
    ,"httpSourceId":"-"
    ,"ruleGroupList":
    [{
        "ruleGroupId":"arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/hello-
world/c05lb698-1f11-4m41-aef4-99a506d53f4b"
        ,"terminatingRule":{
            "ruleId":"RuleA-XSS"
            ,"action":"BLOCK"
            ,"ruleMatchDetails":null
            }
        ,"nonTerminatingMatchingRules":
        [{
            "ruleId":"RuleB-SQLi"
            ,"action":"COUNT"
            ,"ruleMatchDetails":
            [{
                "conditionType":"SQL_INJECTION"
                ,"sensitivityLevel": "LOW"
                ,"location":"HEADER"
                ,"matchedData":[
                    "10"
```

```
                    ,"and"
                    ,"1"]
            }]
        }]
        ,"excludedRules":null
    }]
    ,"rateBasedRuleList":[]
    ,"nonTerminatingMatchingRules":[]
    ,"httpRequest":{
        "clientIp":"3.3.3.3"
        ,"country":"US"
        ,"headers":
        [
            {"name":"Host","value":"localhost:1989"}
            ,{"name":"User-Agent","value":"curl/7.61.1"}
            ,{"name":"Accept","value":"*/*"}
            ,{"name":"myHeader1","value":"<frameset onload=alert(1)>"}
            ,{"name":"myHeader2","value":"10 AND 1=1"}
            ]
        ,"uri":"/myUri"
        ,"args":""
        ,"httpVersion":"HTTP/1.1"
        ,"httpMethod":"GET"
        ,"requestId":"rid"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```

Example Sortie du journal pour une règle déclenchée pour l'inspection du corps de la demande avec le type de contenu JSON

AWS WAF indique actuellement l'emplacement de l'inspection du corps JSON sous la formeUNKNOWN.

```
{
    "timestamp": 1576280412771,
    "formatVersion": 1,
    "webaclId": "arn:aws:wafv2:ap-southeast-2:123456789012:regional/webacl/test/111",
    "terminatingRuleId": "STMTest_SQLi_XSS",
```

```
    "terminatingRuleType": "REGULAR",
    "action": "BLOCK",
    "terminatingRuleMatchDetails": [
        {
            "conditionType": "SQL_INJECTION",
            "sensitivityLevel": "LOW",
            "location": "UNKNOWN",
            "matchedData": [
                "10",
                "AND",
                "1"
            ]
        }
    ],
    "httpSourceName": "ALB",
    "httpSourceId": "alb",
    "ruleGroupList": [],
    "rateBasedRuleList": [],
    "nonTerminatingMatchingRules": [],
    "requestHeadersInserted":null,
    "responseCodeSent":null,
    "httpRequest": {
        "clientIp": "1.1.1.1",
        "country": "AU",
        "headers": [],
        "uri": "",
        "args": "",
        "httpVersion": "HTTP/1.1",
        "httpMethod": "POST",
        "requestId": "null"
    },
    "labels": [
        {
            "name": "value"
        }
    ]
}
```


Example Sortie du journal pour une règle CAPTCHA par rapport à une requête Web avec un jeton CAPTCHA valide et non expiré

La liste de journaux suivante concerne une requête Web correspondant à une règle et à une CAPTCHA action. La requête Web contient un jeton CAPTCHA valide et non expiré, et elle est

uniquement notée comme une correspondance CAPTCHA par AWS WAF, de la même manière que le comportement de l'action. Count Cette correspondance CAPTCHA est indiquée ci-dessous. `nonTerminatingMatchingRules`


```
{
  "timestamp": 1632420429309,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "Default_Action",
  "terminatingRuleType": "REGULAR",
  "action": "ALLOW",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [
    {
      "ruleId": "captcha-rule",
      "action": "CAPTCHA",
      "ruleMatchDetails": [],
      "captchaResponse": {
        "responseCode": 0,
        "solveTimestamp": 1632420429
      }
    }
  ],
  "requestHeadersInserted": [
    {
      "name": "x-amzn-waf-test-header-name",
      "value": "test-header-value"
    }
  ],
  "responseCodeSent": null,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
```

```
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc24d-5ad89a09181910c43917a888"
      },
      {
        "name": "cache-control",
        "value": "max-age=0"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
```

```
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "same-origin"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "referer",
        "value": "https://b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com/pen-
test/pets"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      },
      {
        "name": "cookie",
        "value": "aws-waf-token=51c71352-41f5-4f6d-b676-c24907bdf819:EQoAZ/J
+AAQAAAAA:t9wvxbw042wva7E2Y6lgud/
bS6YG0CJKVAJqaRqDZ140ythKW0Zj9wKB2O8lSkYDRqf1yONcVBFo5u0eYi0tvT4rtQCXsu
+KanAardW8go4QSLw4yoED59lgV7oAhGyCalAzE7ra29j+RvvZPsQyoQuDCrtoY/TvQyMTXIXzGPDC/rKBbg=="
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
```

```
    "requestId": "GINMHHUgoAMFxug="
  }
}
```

Example Sortie du journal pour une règle CAPTCHA par rapport à une requête Web qui ne contient pas de jeton CAPTCHA

La liste de journaux suivante concerne une requête Web correspondant à une règle et à une CAPTCHA action. La requête Web ne comportait pas de jeton CAPTCHA et a été bloquée par. AWS WAF

```
{
  "timestamp": 1632420416512,
  "formatVersion": 1,
  "webaclId": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/captcha-web-
acl/585e38b5-afce-4d2a-b417-14fb08b66c67",
  "terminatingRuleId": "captcha-rule",
  "terminatingRuleType": "REGULAR",
  "action": "CAPTCHA",
  "terminatingRuleMatchDetails": [],
  "httpSourceName": "APIGW",
  "httpSourceId": "123456789012:b34myvfw0b:pen-test",
  "ruleGroupList": [],
  "rateBasedRuleList": [],
  "nonTerminatingMatchingRules": [],
  "requestHeadersInserted": null,
  "responseCodeSent": 405,
  "httpRequest": {
    "clientIp": "72.21.198.65",
    "country": "US",
    "headers": [
      {
        "name": "X-Forwarded-For",
        "value": "72.21.198.65"
      },
      {
        "name": "X-Forwarded-Proto",
        "value": "https"
      },
      {
        "name": "X-Forwarded-Port",
        "value": "443"
      },
```

```
      {
        "name": "Host",
        "value": "b34myvfw0b.gamma.execute-api.us-east-1.amazonaws.com"
      },
      {
        "name": "X-Amzn-Trace-Id",
        "value": "Root=1-614cc240-18b57ff33c10e5c016b508c5"
      },
      {
        "name": "sec-ch-ua",
        "value": "\"Chromium\";v=\"94\", \"Google Chrome\";v=\"94\", \";Not A Brand
\";v=\"99\""
      },
      {
        "name": "sec-ch-ua-mobile",
        "value": "?0"
      },
      {
        "name": "sec-ch-ua-platform",
        "value": "\"Windows\""
      },
      {
        "name": "upgrade-insecure-requests",
        "value": "1"
      },
      {
        "name": "user-agent",
        "value": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/94.0.4606.54 Safari/537.36"
      },
      {
        "name": "accept",
        "value": "text/html,application/xhtml+xml,application/xml;q=0.9,image/
avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9"
      },
      {
        "name": "sec-fetch-site",
        "value": "cross-site"
      },
      {
        "name": "sec-fetch-mode",
        "value": "navigate"
      },
      {
```

```
        "name": "sec-fetch-user",
        "value": "?1"
      },
      {
        "name": "sec-fetch-dest",
        "value": "document"
      },
      {
        "name": "accept-encoding",
        "value": "gzip, deflate, br"
      },
      {
        "name": "accept-language",
        "value": "en-US,en;q=0.9"
      }
    ],
    "uri": "/pen-test/pets",
    "args": "",
    "httpVersion": "HTTP/1.1",
    "httpMethod": "GET",
    "requestId": "GINKHEssoAMFsrg="
  },
  "captchaResponse": {
    "responseCode": 405,
    "solveTimestamp": 0,
    "failureReason": "TOKEN_MISSING"
  }
}
```


Tester et ajuster vos AWS WAF protections

Nous vous recommandons de tester et d'ajuster les modifications apportées à votre ACL AWS WAF Web avant de les appliquer au trafic de votre site Web ou de votre application Web.

⚠ Risque lié au trafic de production

Avant de déployer votre implémentation ACL Web pour le trafic de production, testez-la et ajustez-la dans un environnement intermédiaire ou de test jusqu'à ce que vous soyez à l'aise avec l'impact potentiel sur votre trafic. Testez et ajustez ensuite les règles en mode comptage avec votre trafic de production avant de les activer.

Cette section fournit des conseils pour tester et ajuster vos ACL AWS WAF Web, vos règles, vos groupes de règles, vos ensembles d'adresses IP et vos ensembles de modèles regex.

Cette section fournit également des conseils généraux pour tester votre utilisation de groupes de règles gérés par quelqu'un d'autre. Il s'agit notamment des groupes de règles AWS AWS Marketplace gérées, des groupes de règles gérés et des groupes de règles partagés avec vous par un autre compte. Pour ces groupes de règles, suivez également les instructions fournies par le fournisseur de groupes de règles.

- Pour le groupe de règles AWS gérées par Bot Control, voir égalementTester et déployer AWS WAF Bot Control.
- Pour le groupe de règles de AWS prévention du piratage de comptes, voir égalementTester et déployer ATP.
- Pour le groupe de règles de prévention de la AWS fraude relatif à la création de comptes, voir égalementTest et déploiement de l'ACFP.

Incohérences temporaires lors des mises à jour

Lorsque vous créez ou modifiez une ACL Web ou d'autres AWS WAF ressources, les modifications mettent peu de temps à se propager à toutes les zones où les ressources sont stockées. Le temps de propagation peut aller de quelques secondes à plusieurs minutes.

Voici des exemples d'incohérences temporaires que vous pourriez remarquer lors de la propagation des modifications :

- Après avoir créé une ACL Web, si vous essayez de l'associer à une ressource, vous pouvez obtenir une exception indiquant que l'ACL Web n'est pas disponible.
- Une fois que vous avez ajouté un groupe de règles à une ACL Web, les nouvelles règles de groupe de règles peuvent être en vigueur dans une zone où l'ACL Web est utilisée et pas dans une autre.
- Une fois que vous avez modifié le paramètre d'une action de règle, vous pouvez voir l'ancienne action à certains endroits et la nouvelle action à d'autres.
- Après avoir ajouté une adresse IP à un ensemble d'adresses IP utilisé dans une règle de blocage, la nouvelle adresse peut être bloquée dans une zone alors qu'elle est toujours autorisée dans une autre.

Tester et régler des étapes de haut niveau

Cette section fournit une liste des étapes à suivre pour tester les modifications apportées à votre ACL Web, y compris les règles ou les groupes de règles qu'elle utilise.

> **Note**
>
> Pour suivre les instructions de cette section, vous devez comprendre comment créer et gérer des AWS WAF protections telles que les ACL Web, les règles et les groupes de règles. Ces informations sont abordées dans les sections précédentes de ce guide.

Pour tester et régler votre ACL Web

Effectuez ces étapes d'abord dans un environnement de test, puis en production.

1. Préparez-vous aux tests

   Préparez votre environnement de surveillance, passez vos nouvelles AWS WAF protections en mode comptage pour les tests et créez les associations de ressources dont vous avez besoin.

   veuillez consulter Préparation aux tests.
2. Surveillez et optimisez les environnements de test et de production

   Surveillez et ajustez vos AWS WAF protections d'abord dans un environnement de test ou de préparation, puis en production, jusqu'à ce que vous soyez certain qu'elles peuvent gérer le trafic comme vous le souhaitez.

   veuillez consulter Surveillance et réglage.
3. Activez vos protections en production

   Lorsque vous êtes satisfait de vos protections de test, passez en mode production, nettoyez tous les artefacts de test inutiles et poursuivez la surveillance.

   veuillez consulter Activer vos protections en production.

Une fois que vous avez terminé d'implémenter vos modifications, continuez à surveiller votre trafic Web et les protections en production pour vous assurer qu'elles fonctionnent comme vous le

souhaitez. Les modèles de trafic Web peuvent changer au fil du temps. Il se peut donc que vous deviez ajuster les protections de temps en temps.

Préparation aux tests

Cette section décrit comment configurer pour tester et ajuster vos AWS WAF protections.

> **Note**
>
> Pour suivre les instructions de cette section, vous devez comprendre de manière générale comment créer et gérer des AWS WAF protections telles que les ACL Web, les règles et les groupes de règles. Ces informations sont abordées dans les sections précédentes de ce guide.

Pour préparer les tests

1. Activez la journalisation de l'ACL Web, CloudWatch les métriques Amazon et l'échantillonnage des demandes Web pour l'ACL Web

   Utilisez la journalisation, les métriques et l'échantillonnage pour surveiller l'interaction des règles ACL Web avec votre trafic Web.

   - Journalisation : vous pouvez configurer AWS WAF pour consigner les requêtes Web évaluées par une ACL Web. Vous pouvez envoyer des journaux vers CloudWatch des journaux, un compartiment Amazon S3 ou un flux de diffusion Amazon Data Firehose. Vous pouvez supprimer des champs et appliquer un filtrage. Pour plus d'informations, consultez Journalisation AWS WAF du trafic ACL Web.
   - Amazon Security Lake : vous pouvez configurer Security Lake pour collecter des données ACL Web. Security Lake collecte les données des journaux et des événements à partir de diverses sources à des fins de normalisation, d'analyse et de gestion. Pour plus d'informations sur cette option, consultez Qu'est-ce qu'Amazon Security Lake ? et Collecte de données à partir AWS des services décrits dans le guide de l'utilisateur d'Amazon Security Lake.
   - Amazon CloudWatch metrics — Dans la configuration de votre ACL Web, fournissez des spécifications métriques pour tout ce que vous souhaitez surveiller. Vous pouvez consulter les statistiques via les CloudWatch consoles AWS WAF et. Pour plus d'informations, consultez Surveillance avec Amazon CloudWatch.

- Échantillonnage de requêtes Web : vous pouvez consulter un échantillon de toutes les demandes Web évaluées par votre ACL Web. Pour plus d'informations sur l'échantillonnage des requêtes Web, consultezAffichage d'un exemple de demandes web.

2. Réglez vos protections en Count mode

   Dans la configuration de votre ACL Web, passez tout ce que vous souhaitez tester en mode comptage. Cela permet aux protections de test d'enregistrer les correspondances par rapport aux requêtes Web sans modifier la façon dont les demandes sont traitées. Vous pourrez voir les correspondances dans vos statistiques, vos journaux et vos exemples de demandes, afin de vérifier les critères de correspondance et de comprendre les effets potentiels sur votre trafic Web. Les règles qui ajoutent des étiquettes aux demandes correspondantes ajouteront des étiquettes quelle que soit l'action de la règle.

   - Règle définie dans l'ACL Web — Modifiez les règles dans l'ACL Web et définissez leurs actions surCount.
   - Groupe de règles : dans votre configuration ACL Web, modifiez l'énoncé de règle du groupe de règles et, dans le volet Règles, ouvrez le menu déroulant Remplacer toutes les actions de règles et choisissez. Count Si vous gérez l'ACL Web au format JSON, ajoutez les règles aux `RuleActionOverrides` paramètres de la déclaration de référence du groupe de règles, avec `ActionToUse` set toCount. La liste d'exemples suivante montre les remplacements de deux règles du groupe de règles `AWSManagedRulesAnonymousIpList` AWS Managed Rules.

     ```
     "ManagedRuleGroupStatement": {
       "VendorName": "AWS",
       "Name": "AWSManagedRulesAnonymousIpList",
         "RuleActionOverrides": [
           {
             "ActionToUse": {
               "Count": {}
             },
             "Name": "AnonymousIPList"
           },
           {
             "ActionToUse": {
               "Count": {}
             },
             "Name": "HostingProviderIPList"
           }
     ```

```
      ],
      "ExcludedRules": []
    }
  },
```

Pour plus d'informations sur les dérogations aux actions des règles, consultezRemplacer les actions des règles dans un groupe de règles.

Pour votre propre groupe de règles, ne modifiez pas les actions des règles dans le groupe de règles lui-même. Les règles de groupe de règles avec Count action ne génèrent pas les métriques ou autres artefacts dont vous avez besoin pour vos tests. En outre, la modification d'un groupe de règles affecte toutes les ACL Web qui l'utilisent, tandis que les modifications apportées à la configuration des ACL Web n'affectent que l'unique ACL Web.

- ACL Web — Si vous testez une nouvelle ACL Web, définissez l'action par défaut de l'ACL Web afin d'autoriser les demandes. Cela vous permet d'essayer l'ACL Web sans affecter le trafic de quelque façon que ce soit.

En général, le mode comptage génère plus de correspondances que le mode production. En effet, une règle qui compte les demandes n'arrête pas l'évaluation de la demande par l'ACL Web, de sorte que les règles exécutées ultérieurement dans l'ACL Web peuvent également correspondre à la demande. Lorsque vous modifiez les actions de vos règles en fonction de leurs paramètres de production, les règles qui autorisent ou bloquent les demandes mettent fin à l'évaluation des demandes auxquelles elles correspondent. Par conséquent, les demandes correspondantes seront généralement inspectées selon un nombre réduit de règles dans l'ACL Web. Pour plus d'informations sur les effets des actions liées aux règles sur l'évaluation globale d'une requête Web, consultezAction de la règle.

Avec ces paramètres, vos nouvelles protections ne modifieront pas le trafic Web, mais généreront des informations de correspondance sous forme de métriques, de journaux ACL Web et d'exemples de demandes.

3. Associer l'ACL Web à une ressource

   Si l'ACL Web n'est pas déjà associée à la ressource, associez-la.

   veuillez consulter Associer ou dissocier une ACL Web à une ressource AWS.

Vous êtes maintenant prêt à surveiller et à régler votre ACL Web.

Surveillance et réglage

Cette section explique comment surveiller et régler vos AWS WAF protections.

> **Note**
>
> Pour suivre les instructions de cette section, vous devez comprendre de manière générale comment créer et gérer des AWS WAF protections telles que les ACL Web, les règles et les groupes de règles. Ces informations sont abordées dans les sections précédentes de ce guide.

Surveillez le trafic Web et les correspondances de règles pour vérifier le comportement de l'ACL Web. Si vous rencontrez des problèmes, ajustez vos règles pour les corriger, puis surveillez pour vérifier les ajustements.

Répétez la procédure suivante jusqu'à ce que l'ACL Web gère votre trafic Web comme vous en avez besoin.

Pour surveiller et régler

1. Surveillez le trafic et respectez les règles

   Assurez-vous que le trafic circule et que vos règles de test trouvent les demandes correspondantes.

   Consultez les informations suivantes concernant les protections que vous testez :

   - Journaux : accédez aux informations relatives aux règles qui correspondent à une requête Web :
     - Vos règles : les règles de l'ACL Web qui ont une Count action sont répertoriées ci-dessousnon`TerminatingMatchingRules`. Les règles avec Allow ou Block sont répertoriées sous la forme`terminatingRule`. Les règles avec CAPTCHA ou Challenge peuvent être résilientes ou non, et sont donc répertoriées dans l'une des deux catégories, en fonction du résultat de la correspondance des règles.
     - Groupes de règles : les groupes de règles sont identifiés `ruleGroupId` sur le terrain et leurs correspondances sont classées de la même manière que pour les règles autonomes.
     - Étiquettes : les étiquettes que les règles ont appliquées à la demande sont répertoriées dans le `Labels` champ.

Pour plus d'informations, consultez Champs de journal.

- CloudWatch Métriques Amazon — Vous pouvez accéder aux statistiques suivantes pour évaluer votre demande ACL Web.
  - Vos règles : les métriques sont regroupées en fonction de l'action de la règle. Par exemple, lorsque vous testez une règle en Count mode, ses correspondances sont répertoriées sous forme de `Count` métriques pour l'ACL Web.
  - Vos groupes de règles : les statistiques de vos groupes de règles sont répertoriées sous les métriques des groupes de règles.
  - Groupes de règles appartenant à un autre compte : les statistiques des groupes de règles ne sont généralement visibles que par le propriétaire du groupe de règles. Toutefois, si vous annulez l'action d'une règle, les mesures associées à cette règle seront répertoriées sous les mesures de votre ACL Web. En outre, les étiquettes ajoutées par n'importe quel groupe de règles sont répertoriées dans vos métriques ACL Web

    Les groupes de règles de cette catégorie sont les groupes de règles AWS Règles gérées pour AWS WAF AWS Marketplace groupes de règles gérésGroupes de règles fournis par d'autres services,, et les groupes de règles partagés avec vous par un autre compte.
  - Étiquettes : les étiquettes qui ont été ajoutées à une demande Web lors de l'évaluation sont répertoriées dans les métriques des étiquettes ACL Web. Vous pouvez accéder aux statistiques de toutes les étiquettes, qu'elles aient été ajoutées par vos règles et groupes de règles ou par les règles d'un groupe de règles appartenant à un autre compte.

  Pour plus d'informations, consultez Affichage des métriques pour votre ACL Web.
- Tableaux de bord d'aperçu du trafic Web ACL : accédez aux résumés du trafic Web évalué par une ACL Web en accédant à la page de l'ACL Web dans la AWS WAF console et en ouvrant l'onglet Aperçu du trafic.

  Les tableaux de bord d'aperçu du trafic fournissent des résumés en temps quasi réel des CloudWatch métriques AWS WAF collectées par Amazon lors de l'évaluation du trafic Web de votre application.

  Pour plus d'informations, consultez Tableaux de bord de présentation du trafic Web ACL.
- Demandes Web échantillonnées : accédez aux informations relatives aux règles qui correspondent à un échantillon de requêtes Web. Les exemples d'informations identifient les règles correspondantes par le nom de métrique de la règle dans l'ACL Web. Pour les groupes de règles, la métrique identifie l'énoncé de référence du groupe de règles. Pour les

règles au sein de groupes de règles, l'exemple répertorie le nom de règle correspondant dans`RuleWithinRuleGroup`.

Pour plus d'informations, consultez Affichage d'un exemple de demandes web.

2. Configurer les mesures d'atténuation pour corriger les faux positifs

Si vous déterminez qu'une règle génère des faux positifs, en faisant correspondre les requêtes Web alors qu'elle ne le devrait pas, les options suivantes peuvent vous aider à ajuster vos protections ACL Web afin de les atténuer.

Corriger les critères d'inspection des règles

Pour vos propres règles, il vous suffit souvent d'ajuster les paramètres que vous utilisez pour inspecter les requêtes Web. Les exemples incluent la modification des spécifications d'un ensemble de modèles regex, l'ajustement des transformations de texte que vous appliquez à un composant de demande avant l'inspection ou le passage à l'utilisation d'une adresse IP transférée. Consultez les instructions relatives au type de règle à l'origine des problèmes, sousNotions de base sur les énoncés.

Corriger des problèmes plus complexes

Pour les critères d'inspection que vous ne contrôlez pas et pour certaines règles complexes, vous devrez peut-être apporter d'autres modifications, par exemple en ajoutant des règles qui autorisent ou bloquent explicitement les demandes ou qui éliminent les demandes de l'évaluation par la règle problématique. Les groupes de règles gérés ont le plus souvent besoin de ce type d'atténuation, mais d'autres règles le peuvent également. Les exemples incluent l'instruction de règle basée sur le débit et l'instruction de règle d'attaque par injection SQL.

Les mesures à prendre pour atténuer les faux positifs dépendent de votre cas d'utilisation. Les approches les plus courantes sont les suivantes :

- Ajouter une règle atténuante : ajoutez une règle qui s'exécute avant la nouvelle règle et qui autorise explicitement les demandes qui génèrent des faux positifs. Pour plus d'informations sur l'ordre d'évaluation des règles dans une ACL Web, consultezOrdre de traitement des règles et des groupes de règles dans une ACL Web.

  Avec cette approche, les demandes autorisées sont envoyées à la ressource protégée, de sorte qu'elles n'atteignent jamais la nouvelle règle d'évaluation. Si la nouvelle règle est un

groupe de règles géré payant, cette approche peut également contribuer à limiter le coût d'utilisation du groupe de règles.

- Ajouter une règle logique avec une règle atténuante : utilisez des instructions de règle logique pour combiner la nouvelle règle avec une règle qui exclut les faux positifs. Pour plus d'informations, consultez Déclarations de règles logiques.

  Supposons, par exemple, que vous ajoutiez une instruction SQL Attack Match qui génère des faux positifs pour une catégorie de requêtes. Créez une règle qui correspond à ces demandes, puis combinez les règles à l'aide d'instructions de règles logiques afin de ne faire correspondre que les demandes qui ne répondent pas aux critères des faux positifs et qui répondent aux critères des attaques par injection SQL.

- Ajouter une instruction de portée réduite : pour les instructions basées sur le taux et les instructions de référence à des groupes de règles gérés, excluez les demandes qui génèrent des faux positifs de l'évaluation en ajoutant une instruction de portée réduite dans l'instruction principale.

  Une demande qui ne correspond pas à l'instruction scope-down n'atteint jamais le groupe de règles ou l'évaluation basée sur le taux. Pour plus d'informations sur les instructions de portée réduite, consultez. Déclarations de portée réduite Pour obtenir un exemple, consultez Exclure la plage d'adresses IP de la gestion des robots.

- Ajouter une règle de correspondance des libellés : pour les groupes de règles qui utilisent l'étiquetage, identifiez l'étiquette que la règle problématique applique aux demandes. Vous devrez peut-être d'abord définir les règles du groupe de règles en mode décompte, si ce n'est déjà fait. Ajoutez une règle de correspondance des libellés, positionnée pour s'exécuter après le groupe de règles, qui correspond à l'étiquette ajoutée par la règle problématique. Dans la règle de correspondance des libellés, vous pouvez filtrer les demandes que vous souhaitez autoriser de celles que vous souhaitez bloquer.

  Si vous utilisez cette approche, lorsque vous aurez terminé le test, conservez la règle problématique en mode décompte dans le groupe de règles et maintenez votre règle de correspondance d'étiquettes personnalisée en place. Pour plus d'informations sur les déclarations de correspondance des étiquettes, voirDéclaration relative à la règle de correspondance des étiquettes. Pour obtenir des exemples, veuillez consulter Autoriser un bot bloqué spécifique et Exemple ATP : gestion personnalisée des informations d'identification manquantes ou compromises.

- Modifier la version d'un groupe de règles géré : pour les groupes de règles gérés versionnés, modifiez la version que vous utilisez. Par exemple, vous pouvez revenir à la dernière version statique que vous avez utilisée avec succès.

  Il s'agit généralement d'une solution temporaire. Vous pouvez modifier la version pour votre trafic de production pendant que vous continuez à tester la dernière version dans votre environnement de test ou de préparation, ou pendant que vous attendez une version plus compatible de la part du fournisseur. Pour plus d'informations sur les versions des groupes de règles gérés, consultezGroupes de règles gérés.

Lorsque vous êtes certain que les nouvelles règles correspondent aux demandes comme vous le souhaitez, passez à l'étape suivante de vos tests et répétez cette procédure. Effectuez la dernière étape de test et de réglage dans votre environnement de production.

Affichage des métriques pour votre ACL Web

Après avoir associé une ACL Web à une ou plusieurs AWS ressources, vous pouvez consulter les statistiques obtenues pour l'association dans un CloudWatch graphique Amazon.

Pour plus d'informations sur AWS WAF les métriques, consultezAWS WAF métriques et dimensions. Pour plus d'informations sur CloudWatch les métriques, consultez le guide de CloudWatch l'utilisateur Amazon.

Pour chacune de vos règles dans une ACL Web et pour toutes les demandes qu'une ressource associée transmet à AWS WAF une ACL Web, vous CloudWatch pouvez effectuer les opérations suivantes :

- Afficher les données de l'heure précédente ou des trois heures précédentes.
- Modifiez l'intervalle entre les points de données.
- Modifiez le calcul effectué sur CloudWatch les données, tel que le maximum, le minimum, la moyenne ou la somme.

> **Note**
>
> AWS WAF with CloudFront est un service mondial et les statistiques ne sont disponibles que lorsque vous choisissez la région USA Est (Virginie du Nord) dans le AWS Management

Console. Si vous choisissez une autre région, aucune AWS WAF métrique n'apparaîtra dans la CloudWatch console.

Pour afficher les données des règles d'une liste ACL web

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Si nécessaire, remplacez la région par celle où se trouvent vos AWS ressources. Pour CloudFront, choisissez la région USA Est (Virginie du Nord).
3. Dans le volet de navigation, sous Mesures, sélectionnez Toutes les mesures, puis recherchez dans l'onglet Parcourir pour`AWS::WAFV2`.
4. Cochez la case de la liste ACL web dont vous voulez afficher les données.
5. Modifiez les paramètres applicables :

   Statistique

   Choisissez le calcul à CloudWatch effectuer sur les données.

   Plage horaire

   Choisissez si vous souhaitez afficher les données de la dernière heure ou des trois dernières heures.

   Période

   Choisissez l'intervalle entre les points de données sur le graphique.

   Règles

   Choisissez les règles dont vous souhaitez afficher les données.

   > **Note**
   >
   > Si vous modifiez le nom d'une règle et que vous souhaitez que le nom de la métrique de la règle reflète le changement, vous devez également mettre à jour le nom de la métrique. AWS WAF ne met pas automatiquement à jour le nom de la métrique d'une règle lorsque vous modifiez le nom de la règle. Vous pouvez modifier le nom de la métrique lorsque vous modifiez la règle dans la console, à l'aide de l'éditeur JSON de

règles. Vous pouvez également modifier les deux noms via les API et dans toute liste JSON que vous utilisez pour définir votre ACL Web ou votre groupe de règles.

Notez ce qui suit :

- Si vous avez récemment associé une ACL Web à une AWS ressource, vous devrez peut-être attendre quelques minutes pour que les données apparaissent dans le graphique et que la métrique de l'ACL Web apparaisse dans la liste des métriques disponibles.
- Si vous associez plusieurs ressources à une ACL Web, les CloudWatch données incluront les demandes pour chacune d'entre elles.
- Vous pouvez placer le curseur sur un point de données pour obtenir plus d'informations.
- Le graphique n'est pas actualisé automatiquement. Pour mettre à jour l'affichage, cliquez sur l'icône
  ().

Pour plus d'informations sur CloudWatch les métriques, consultezSurveillance avec Amazon CloudWatch.

Tableaux de bord de présentation du trafic Web ACL

Cette section décrit les tableaux de bord de présentation du trafic ACL Web dans la AWS WAF console. Après avoir associé une ACL Web à une ou plusieurs AWS ressources et activé les métriques pour l'ACL Web, vous pouvez accéder aux résumés du trafic Web évalué par l'ACL Web en accédant à l'onglet Aperçu du trafic de l'ACL Web dans la AWS WAF console. Les tableaux de bord incluent des résumés en temps quasi réel des CloudWatch statistiques Amazon AWS WAF collectées lors de l'évaluation du trafic Web de votre application.

> **Note**
>
> Si vous ne voyez rien sur les tableaux de bord, assurez-vous que les métriques sont activées pour l'ACL Web.

L'onglet Aperçu du trafic de l'ACL Web contient des tableaux de bord à onglets contenant les catégories d'informations suivantes :

- Tout le trafic : toutes les demandes Web évaluées par l'ACL Web.

  Le tableau de bord met l'accent sur la fin des actions, mais vous pouvez consulter les correspondances aux règles de décompte aux emplacements suivants :

  - Panneau des 10 meilleures règles de ce tableau de bord. Activez l'action Basculer vers le comptage pour afficher les correspondances aux règles de comptage.
  - Onglet de demandes échantillonnées de la page Web ACL. Ce nouvel onglet inclut un graphique de toutes les règles correspondantes. Pour plus d'informations, consultez Affichage d'un exemple de demandes web.
- Contrôle des robots : demandes Web que l'ACL Web évalue à l'aide du groupe de règles géré par le contrôle des robots.

  Si vous n'utilisez pas ce groupe de règles dans votre ACL Web, cet onglet affiche les résultats de l'évaluation d'un échantillon de votre trafic Web par rapport aux règles de contrôle des robots. Cela vous donne une idée du trafic de bots que reçoit votre application et c'est gratuit.

  Ce groupe de règles fait partie des options intelligentes d'atténuation des menaces AWS WAF proposées. Pour plus d'informations, consultez AWS WAF Contrôle des robots et AWS WAF Groupe de règles Bot Control.
- Prévention du piratage de compte — Le Web demande à l'ACL Web d'évaluer à l'aide du groupe de règles géré par AWS WAF Fraud Control Account Takeover Prevention (ATP). Cet onglet n'est disponible que si vous utilisez ce groupe de règles dans votre ACL Web.

  Le groupe de règles ATP fait partie des offres d'atténuation AWS WAF intelligente des menaces. Pour plus d'informations, consultez AWS WAF Contrôle des fraudes et prévention des prises de contrôle des comptes (ATP) et AWS WAF Groupe de règles de prévention des prises de contrôle des fraudes (ATP).
- Prévention de la fraude lors de la création de comptes : requêtes Web que l'ACL Web évalue à l'aide du groupe de règles géré AWS WAF Fraud Control pour la prévention de la fraude à la création de comptes (ACFP). Cet onglet n'est disponible que si vous utilisez ce groupe de règles dans votre ACL Web.

  Le groupe de règles ACFP fait partie des offres d'atténuation AWS WAF intelligente des menaces. Pour plus d'informations, consultez AWS WAF Contrôle des fraudes : création de comptes, prévention des fraudes (ACFP) et AWS WAF Groupe de règles de prévention des fraudes (ACFP) pour la création de comptes et la prévention des fraudes.

Les tableaux de bord sont basés sur les CloudWatch métriques de l'ACL Web, et les graphiques permettent d'accéder aux métriques correspondantes dans CloudWatch. Pour les tableaux de bord intelligents d'atténuation des menaces, tels que Bot Control, les mesures utilisées sont principalement les mesures d'étiquetage.

- Pour obtenir la liste des métriques AWS WAF fournies, consultezAWS WAF métriques et dimensions.
- Pour plus d'informations sur CloudWatch les métriques, consultez le guide de CloudWatch l'utilisateur Amazon.

Les tableaux de bord fournissent des résumés de vos modèles de trafic pour les actions de résiliation et la plage de dates que vous sélectionnez. Les tableaux de bord intelligents d'atténuation des menaces incluent les demandes évaluées par le groupe de règles géré correspondant, que le groupe de règles géré lui-même ait appliqué ou non l'action de résiliation. Par exemple, si cette option Block est sélectionnée, le tableau de bord de prévention du piratage de compte inclut des informations sur toutes les demandes Web qui ont été évaluées par le groupe de règles géré par ATP et bloquées à un moment donné lors de l'évaluation de l'ACL Web. Les demandes peuvent être bloquées par le groupe de règles géré par ATP, par une règle exécutée après le groupe de règles dans l'ACL Web ou par l'action par défaut de l'ACL Web.

Afficher les tableaux de bord d'une ACL Web

Suivez la procédure décrite dans cette section pour accéder aux tableaux de bord ACL Web et définir les critères de filtrage des données. Si vous avez récemment associé une ACL Web à une AWS ressource, vous devrez peut-être attendre quelques minutes pour que les données soient disponibles dans les tableaux de bord.

Les tableaux de bord incluent les demandes pour toutes les ressources que vous avez associées à l'ACL Web.

Pour consulter les tableaux de bord d'aperçu du trafic pour une ACL Web

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, choisissez Web ACL, puis recherchez l'ACL Web qui vous intéresse.
3. Sélectionnez l'ACL Web. La console vous amène à la page de l'ACL Web. L'onglet Aperçu du trafic est sélectionné par défaut.
4. Modifiez les paramètres des filtres de données selon vos besoins.

- Mettre fin aux actions relatives aux règles : sélectionnez les actions de résiliation à inclure dans les tableaux de bord. Les tableaux de bord résument les mesures relatives aux requêtes Web auxquelles l'une des actions sélectionnées a été appliquée lors de l'évaluation de l'ACL Web. Si vous sélectionnez toutes les actions disponibles, les tableaux de bord incluent toutes les requêtes Web évaluées. Pour plus d'informations sur les actions, consultezComment AWS WAF gère les règles et les actions de groupes de règles dans une ACL Web.
- Plage de temps : sélectionnez l'intervalle de temps à afficher dans les tableaux de bord. Vous pouvez choisir d'afficher une période relative au moment présent, par exemple les 3 dernières heures ou la dernière semaine, et vous pouvez sélectionner une plage de temps absolue dans un calendrier.
- Fuseau horaire : ce paramètre s'applique lorsque vous spécifiez une plage de temps absolue. Vous pouvez utiliser le fuseau horaire local de votre navigateur ou le temps universel coordonné (UTC).

Passez en revue les informations figurant dans les onglets qui vous intéressent. Les sélections de filtres de données s'appliquent à tous les tableaux de bord. Dans les volets graphiques, vous pouvez placer le curseur sur un point de données ou une zone pour afficher des détails supplémentaires.

Countrègles d'action

Vous pouvez consulter les informations relatives aux matchs par action de comptage à l'un des deux endroits suivants.

- Dans cet onglet Aperçu du trafic, sur le tableau de bord de l'ensemble du trafic, recherchez le volet des 10 meilleures règles et activez Switch to count action. Lorsque cette option est activée, le volet affiche le nombre de correspondances de règles au lieu de mettre fin aux correspondances de règles.
- Dans l'onglet Demandes échantillonnées de l'ACL Web, consultez un graphique de toutes les correspondances de règles et actions pour la plage de temps que vous avez définie dans l'onglet Aperçu du trafic. Pour plus d'informations sur l'onglet Demandes échantillonnées, consultezAffichage d'un exemple de demandes web.

CloudWatch Métriques Amazon

Dans les volets graphiques du tableau de bord, vous pouvez accéder aux CloudWatch métriques des données graphiques. Choisissez l'option en haut du volet graphique ou dans le menu déroulant (ellipses verticales) situé à l'intérieur du volet.

Actualisation des tableaux de bord

Les tableaux de bord ne sont pas actualisés automatiquement. Pour mettre à jour l'affichage, cliquez sur l'  icône d'actualisation.

Exemples de tableaux de bord d'aperçu du trafic pour les ACL Web

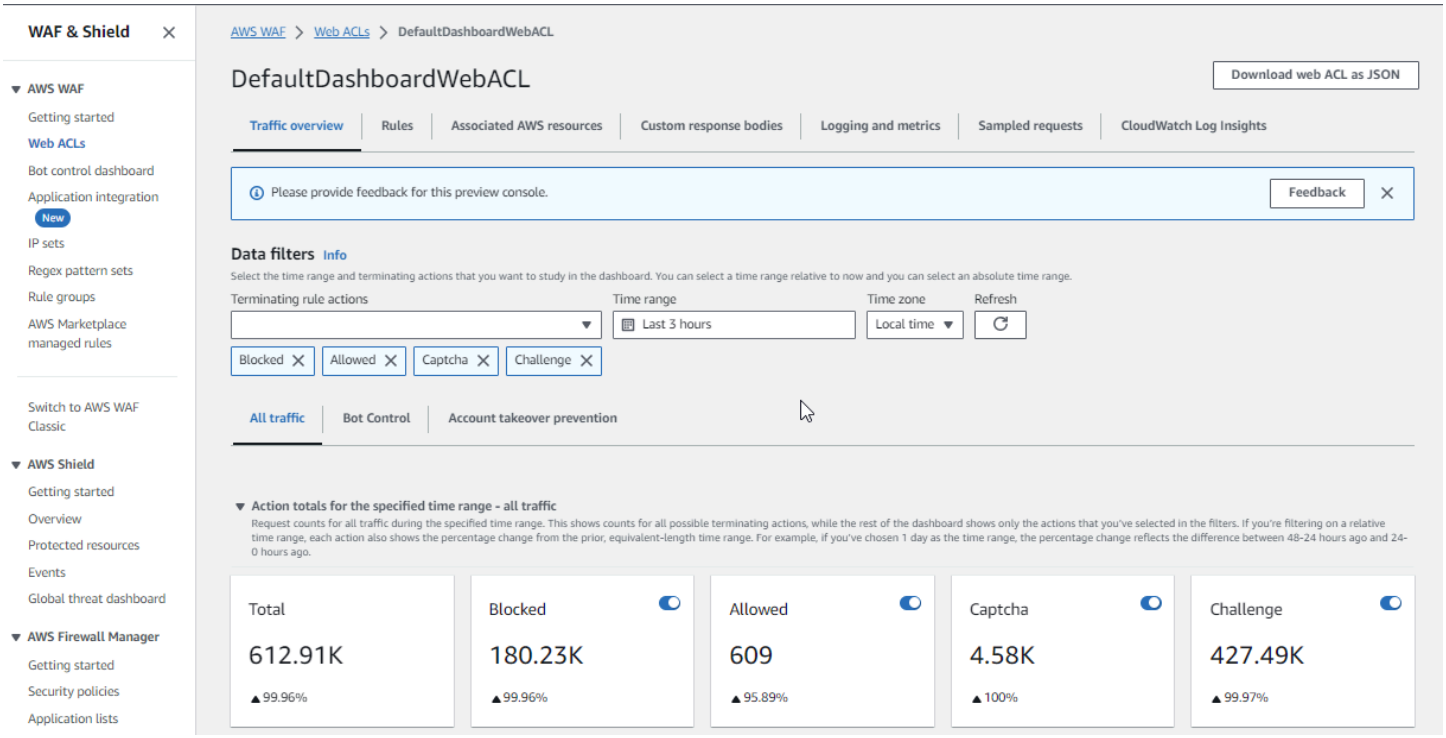
Cette section présente des exemples d'écrans de tableaux de bord d'aperçu du trafic pour les ACL Web.

> **Note**
>
> Si vous les utilisez déjà AWS WAF pour protéger les ressources de votre application, vous pouvez consulter les tableaux de bord de chacune de vos ACL Web sur la page correspondante de la AWS WAF console. Pour plus d'informations, consultez Afficher les tableaux de bord d'une ACL Web.

Exemple d'écran : filtres de données et nombre d'actions du tableau de bord pour l'ensemble du trafic

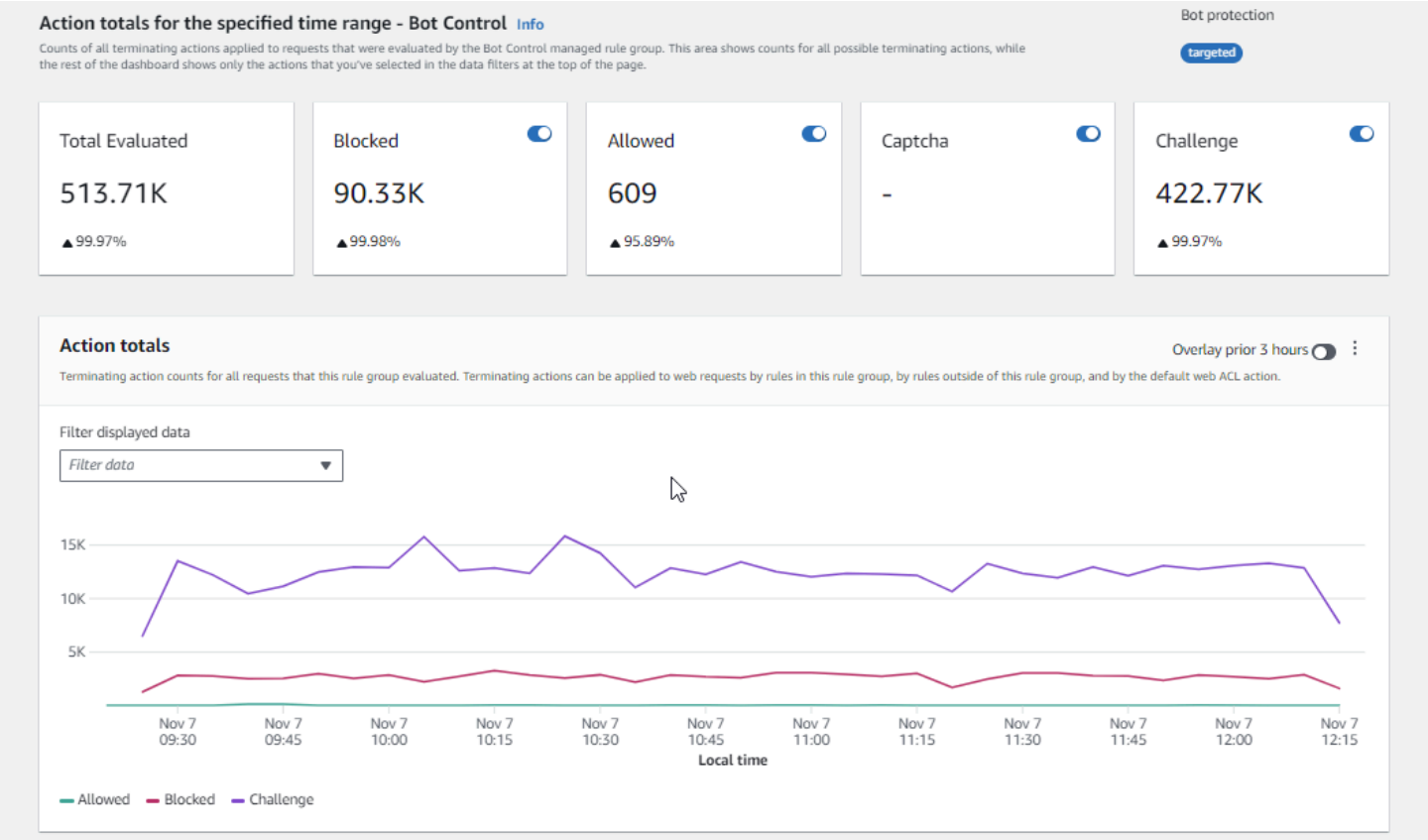
La capture d'écran suivante montre l'aperçu du trafic pour une ACL Web avec l'onglet Tout le trafic sélectionné. Les filtres de données sont définis sur les valeurs par défaut : toutes les actions ont été interrompues au cours des trois dernières heures.

Le tableau de bord de l'ensemble du trafic contient le total des actions pour les différentes actions de terminaison. Chaque volet répertorie le nombre de demandes et affiche une flèche haut/bas indiquant le changement depuis la période de trois heures précédente.



Exemple d'écran : nombre d'actions du tableau de bord Bot Control

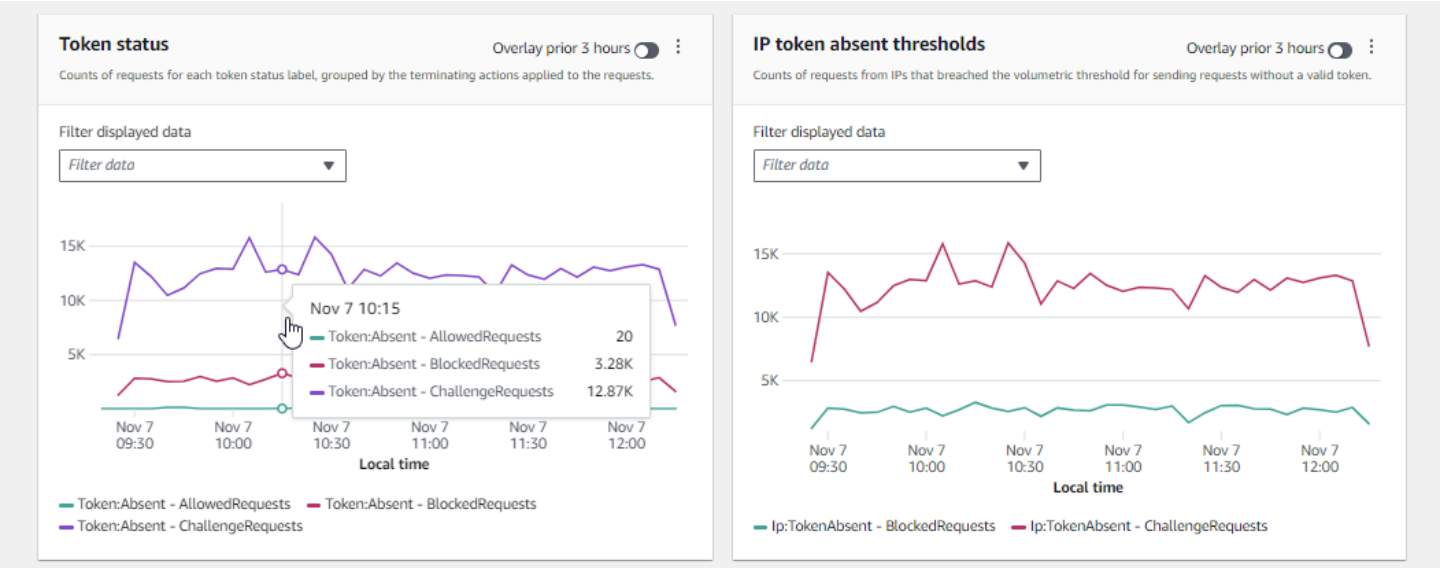
La capture d'écran suivante montre le nombre d'actions pour le tableau de bord Bot Control. Cela affiche les mêmes volets de totaux pour la plage de temps, mais les dénombrements concernent uniquement les demandes évaluées par le groupe de règles Bot Control. Plus bas, dans le volet Total des actions, vous pouvez voir le nombre d'actions pendant la période de trois heures spécifiée. Pour cette plage de temps, l'CAPTCHAaction n'a été appliquée à aucune des demandes évaluées par le groupe de règles.



Exemple d'écran : graphiques récapitulatifs de l'état des jetons du tableau de bord Bot Control

La capture d'écran suivante illustre deux des graphiques récapitulatifs disponibles dans le tableau de bord Bot Control. Le volet État du jeton indique le nombre des différentes étiquettes d'état du jeton, associé à l'action de règle appliquée à la demande. Le volet des seuils d'absence de jeton IP affiche les données relatives aux demandes provenant d'adresses IP qui envoyaient trop de demandes sans jeton.

Le survol d'une zone du graphique permet d'afficher les informations détaillées disponibles. Dans le volet d'état du jeton de cette capture d'écran, la souris survole un point dans le temps, sans se trouver sur aucune ligne graphique. La console affiche donc les données de toutes les lignes à ce moment-là.



Cette section ne présente que quelques-uns des résumés du trafic fournis dans les tableaux de bord d'aperçu du trafic ACL Web. Pour voir les tableaux de bord de l'une de vos ACL Web, ouvrez la page de l'ACL Web dans la console. Pour plus d'informations sur la procédure à suivre, consultez les instructions à l'adresseAfficher les tableaux de bord d'une ACL Web.

Affichage d'un exemple de demandes web

Cette section décrit l'onglet Web ACL Sampled requests de la AWS WAF console. Dans cet onglet, vous pouvez afficher un graphique de toutes les correspondances de règles pour les requêtes Web qui ont AWS WAF été inspectées. En outre, si l'échantillonnage des demandes est activé pour l'ACL Web, vous pouvez consulter un tableau d'un échantillon des demandes Web inspectées. AWS WAF Vous pouvez également récupérer des informations de demande échantillonnées via l'appel `GetSampledRequests` d'API.

L'échantillon de demandes contient jusqu'à 100 demandes correspondant aux critères d'une règle dans l'ACL Web et 100 autres demandes pour lesquelles l'action par défaut de l'ACL Web a été appliquée. Les demandes de l'exemple proviennent de toutes les ressources protégées qui ont reçu des demandes concernant votre contenu au cours des trois heures précédentes.

Lorsqu'une demande Web correspond aux critères d'une règle et que l'action associée à cette règle ne met pas fin à l'évaluation de la demande, AWS WAF continue à inspecter la demande Web en utilisant les règles suivantes de l'ACL Web. De ce fait, une requête Web peut apparaître plusieurs fois. Pour plus d'informations sur les comportements liés à l'action des règles, consultezAction de la règle.

Pour afficher le graphique de toutes les règles et les demandes échantillonnées

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, choisissez Web ACLs.
3. Choisissez le nom de l'ACL Web pour laquelle vous souhaitez consulter les demandes. La console vous amène à la description de la liste ACL web, où vous pouvez la modifier.
4. Dans l'onglet Demandes échantillonnées, vous pouvez voir ce qui suit :

   - Graphique de toutes les règles : ce graphique montre les règles correspondantes et les actions de règles pour toutes les évaluations de requêtes Web effectuées au cours de la période indiquée.

     > **Note**
     >
     > La plage de temps pour ce graphique est définie dans l'onglet Aperçu du trafic de l'ACL Web, dans la section Filtres de données. Pour plus d'informations, veuillez consulter Afficher les tableaux de bord d'une ACL Web.

   - Tableau des demandes échantillonnées : ce tableau affiche les données des demandes échantillonnées pour les 3 dernières heures. Pour chaque entrée, le tableau affiche les données suivantes :

     Nom de la métrique

     Nom de la CloudWatch métrique de la règle dans l'ACL Web qui correspond à la demande. Si une requête Web ne correspond à aucune règle de l'ACL Web, cette valeur est définie par défaut.

     > **Note**
     >
     > Si vous modifiez le nom d'une règle et que vous souhaitez que le nom de la métrique de la règle reflète le changement, vous devez également mettre à jour le nom de la métrique. AWS WAF ne met pas automatiquement à jour le nom de la métrique d'une règle lorsque vous modifiez le nom de la règle. Vous pouvez modifier le nom de la métrique lorsque vous modifiez la règle dans la console, à l'aide de l'éditeur JSON de règles. Vous pouvez également modifier les deux noms

via les API et dans toute liste JSON que vous utilisez pour définir votre ACL Web ou votre groupe de règles.

IP Source

Soit l'adresse IP d'origine de la demande, soit, si le lecteur a utilisé un proxy HTTP ou un Application Load Balancer pour envoyer la demande, l'adresse IP du proxy ou de l'Application Load Balancer.

URI

La partie d'une URL qui identifie une ressource, par exemple, `/images/daily-ad.jpg`.

Règle au sein d'un groupe de règles

Si le nom de la métrique identifie une déclaration de référence de groupe de règles, cela identifie la règle au sein du groupe de règles qui correspond à la demande.

Action

Indique l'action pour la règle correspondante. Pour plus d'informations sur les actions de règle possibles, consultezAction de la règle.

Heure

Heure à laquelle la demande de la ressource protégée AWS WAF a été reçue.

Pour afficher des informations supplémentaires sur les composants d'une requête Web, choisissez le nom de l'URI dans la ligne de la demande.

Activer vos protections en production

Lorsque vous avez terminé la dernière étape de test et de réglage de votre environnement de production, activez vos protections en mode production.

⚠ Risque lié au trafic de production

Avant de déployer votre implémentation ACL Web pour le trafic de production, testez-la et ajustez-la dans un environnement de test jusqu'à ce que vous soyez à l'aise avec l'impact

potentiel sur votre trafic. Testez et réglez-le également en mode comptage avec votre trafic de production avant d'activer vos protections pour le trafic de production.

> **Note**
>
> Pour suivre les instructions de cette section, vous devez comprendre de manière générale comment créer et gérer des AWS WAF protections telles que les ACL Web, les règles et les groupes de règles. Ces informations sont abordées dans les sections précédentes de ce guide.

Effectuez ces étapes d'abord dans votre environnement de test, puis en production.

Activez vos AWS WAF protections en production

1. Passez à vos protections de production

   Mettez à jour votre ACL Web et modifiez vos paramètres de production.

   a. Supprimez toutes les règles de test dont vous n'avez pas besoin

      Si vous avez ajouté des règles de test dont vous n'avez pas besoin en production, supprimez-les. Si vous utilisez des règles de correspondance d'étiquettes pour filtrer les résultats des règles de groupes de règles gérés, veillez à les laisser en place.

   b. Passez aux actions de production

      Modifiez les paramètres d'action de vos nouvelles règles en fonction des paramètres de production prévus.

      - Règle définie dans l'ACL Web — Modifiez les règles dans l'ACL Web et remplacez leurs actions par Count des actions de production.
      - Groupe de règles : dans votre configuration ACL Web du groupe de règles, changez de règle pour qu'elle utilise ses propres actions ou laissez-leur la priorité sur les Count actions, en fonction des résultats de vos activités de test et de réglage. Si vous utilisez une règle de correspondance d'étiquettes pour filtrer les résultats d'une règle de groupe de règles, veillez à laisser la dérogation à cette règle en place.

Pour passer à l'utilisation de l'action d'une règle, dans votre configuration ACL Web, modifiez l'instruction de règle pour le groupe de règles et supprimez la Count dérogation pour la règle. Si vous gérez l'ACL Web au format JSON, dans l'instruction de référence du groupe de règles, supprimez l'entrée correspondant à la règle de la `RuleActionOverrides` liste.

- ACL Web — Si vous avez modifié l'action ACL Web par défaut pour vos tests, réglez-la sur son paramètre de production.

Avec ces paramètres, vos nouvelles protections géreront le trafic Web comme vous le souhaitez.

Lorsque vous enregistrez votre ACL Web, les ressources auxquelles elle est associée utilisent vos paramètres de production.

2. Surveiller et régler

   Pour vous assurer que les requêtes Web sont traitées comme vous le souhaitez, surveillez attentivement votre trafic après avoir activé la nouvelle fonctionnalité. Vous surveillerez les métriques et les journaux relatifs à vos actions relatives aux règles de production, au lieu du nombre d'actions que vous surveilliez dans le cadre de vos travaux de réglage. Continuez à surveiller et ajustez le comportement selon les besoins pour vous adapter à l'évolution de votre trafic Web.

Comment AWS WAF fonctionne avec les CloudFront fonctionnalités d'Amazon

Lorsque vous créez une ACL Web, vous pouvez spécifier une ou plusieurs CloudFront distributions que vous AWS WAF souhaitez inspecter. AWS WAF commence à inspecter et à gérer les demandes Web pour ces distributions en fonction des critères que vous identifiez dans l'ACL Web. CloudFront fournit certaines fonctionnalités qui améliorent les AWS WAF fonctionnalités. Ce chapitre décrit quelques méthodes que vous pouvez configurer CloudFront pour améliorer votre AWS WAF collaboration CloudFront et votre collaboration.

Rubriques

- Utilisation AWS WAF de with CloudFront pour les applications exécutées sur votre propre serveur HTTP
- Choix des méthodes HTTP qui CloudFront répondent à

Utilisation AWS WAF avec des pages d'erreur CloudFront personnalisées

Par défaut, lorsque vous AWS WAF bloquez une requête Web en fonction des critères que vous spécifiez, elle renvoie le code `403 (Forbidden)` d'état HTTP à et le CloudFront renvoie au lecteur. CloudFront Le visualiseur affiche ensuite un message par défaut bref et peu formaté, semblable au suivant :

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

Vous pouvez modifier ce comportement dans vos règles ACL AWS WAF Web en définissant des réponses personnalisées. Pour plus d'informations sur la personnalisation du comportement des réponses à l'aide de AWS WAF règles, consultezRéponses personnalisées pour les Block actions.

> **Note**
>
> Les réponses que vous personnalisez à l'aide de AWS WAF règles ont priorité sur les spécifications de réponse que vous définissez dans les pages d'erreur CloudFront personnalisées.

Si vous préférez afficher un message d'erreur personnalisé CloudFront, éventuellement en utilisant le même format que le reste de votre site Web, vous pouvez configurer CloudFront pour renvoyer au lecteur un objet (par exemple, un fichier HTML) contenant votre message d'erreur personnalisé.

> **Note**
>
> CloudFront Impossible de faire la distinction entre un code d'état HTTP 403 renvoyé par votre origine et un code renvoyé AWS WAF lorsqu'une requête est bloquée. Par conséquent, vous ne pouvez pas renvoyer différentes pages d'erreur personnalisées en fonction des différentes causes d'un code de statut HTTP 403.

Pour plus d'informations sur les pages d'erreur CloudFront personnalisées, consultez la section Génération de réponses d'erreur personnalisées dans le manuel Amazon CloudFront Developer Guide.

Utilisation AWS WAF de with CloudFront pour les applications exécutées sur votre propre serveur HTTP

Lorsque vous l'utilisez AWS WAF CloudFront, vous pouvez protéger vos applications exécutées sur n'importe quel serveur Web HTTP, qu'il s'agisse d'un serveur Web exécuté dans Amazon Elastic Compute Cloud (Amazon EC2) ou d'un serveur Web que vous gérez en privé. Vous pouvez également configurer CloudFront pour exiger le protocole HTTPS entre CloudFront et votre propre serveur Web, ainsi qu'entre les utilisateurs et CloudFront.

Exiger le protocole HTTPS entre CloudFront et votre propre serveur Web

Pour exiger le protocole HTTPS entre votre propre serveur Web CloudFront et votre propre serveur Web, vous pouvez utiliser la fonctionnalité d'origine CloudFront personnalisée et configurer la politique du protocole d'origine et les paramètres du nom de domaine d'origine pour des origines spécifiques. Dans votre CloudFront configuration, vous pouvez spécifier le nom DNS du serveur ainsi que le port et le protocole que vous souhaitez utiliser CloudFront pour récupérer des objets depuis votre origine. Vous devez également vous assurer que le certificat SSL/TLS sur votre serveur d'origine personnalisé correspond au nom de domaine d'origine que vous avez configuré. Lorsque vous utilisez votre propre serveur Web HTTP en dehors de AWS, vous devez utiliser un certificat signé par une autorité de certification (CA) tierce de confiance, par exemple Comodo ou DigiCert Symantec. Pour plus d'informations sur l'exigence du protocole HTTPS pour les communications entre votre propre serveur Web CloudFront et votre propre serveur Web, consultez la rubrique Exiger le protocole HTTPS pour la communication entre CloudFront et votre origine personnalisée dans le manuel Amazon CloudFront Developer Guide.

Exiger le protocole HTTPS entre un utilisateur et CloudFront

Pour exiger le protocole HTTPS entre les spectateurs et CloudFront, vous pouvez modifier la politique du protocole de visionnage pour un ou plusieurs comportements de cache dans votre CloudFront distribution. Pour plus d'informations sur l'utilisation du protocole HTTPS entre utilisateurs CloudFront, consultez la rubrique Requirement du protocole HTTPS pour la communication entre utilisateurs et CloudFront dans le manuel Amazon CloudFront Developer Guide. Vous pouvez également apporter votre propre certificat SSL afin que les utilisateurs puissent se connecter à votre CloudFront distribution via HTTPS en utilisant votre propre nom de domaine, par exemple https://

www.mysite.com. Pour plus d'informations, consultez la rubrique Configuration des noms de domaine alternatifs et du protocole HTTPS dans le manuel Amazon CloudFront Developer Guide.

Choix des méthodes HTTP qui CloudFront répondent à

Lorsque vous créez une distribution CloudFront Web Amazon, vous choisissez les méthodes HTTP que vous CloudFront souhaitez traiter et transmettre à votre source. Choisissez parmi les options suivantes :

- **`GET`**, **`HEAD`** — Vous ne pouvez l'utiliser CloudFront que pour récupérer des objets depuis votre origine ou pour obtenir des en-têtes d'objets.
- **`GET`**,**`HEAD`**, **`OPTIONS`** — Vous CloudFront ne pouvez l'utiliser que pour obtenir des objets depuis votre origine, obtenir des en-têtes d'objets ou récupérer une liste des options prises en charge par votre serveur d'origine.
- **`GET`**,**`HEAD`**,,**`OPTIONS`**,**`PUT`**, **`POSTPATCH`**, **`DELETE`** — Vous pouvez l'utiliser CloudFront pour obtenir, ajouter, mettre à jour et supprimer des objets, ainsi que pour obtenir des en-têtes d'objets. En outre, vous pouvez effectuer d'autres `POST` opérations, telles que l'envoi de données à partir d'un formulaire Web.

Vous pouvez également utiliser des instructions de règle de correspondance des AWS WAF octets pour autoriser ou bloquer les demandes en fonction de la méthode HTTP, comme décrit dansInstruction de correspondance de chaîne de règle. Si vous souhaitez utiliser une combinaison de méthodes compatibles CloudFront , telles que `GET` et`HEAD`, vous n'avez pas besoin de configurer AWS WAF pour bloquer les demandes utilisant les autres méthodes. Si vous souhaitez autoriser une combinaison de méthodes non CloudFront compatibles, telles que, et `GET HEADPOST`, vous pouvez configurer CloudFront pour répondre à toutes les méthodes, puis utiliser AWS WAF pour bloquer les demandes utilisant d'autres méthodes.

Pour plus d'informations sur le choix des méthodes qui CloudFront répondent, consultez la section Méthodes HTTP autorisées dans la rubrique Valeurs que vous spécifiez lors de la création ou de la mise à jour d'une distribution Web du manuel Amazon CloudFront Developer Guide.

Sécurité lors de votre utilisation du AWS WAF service

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

> **Note**
>
> Cette section fournit des conseils AWS de sécurité standard pour votre utilisation du AWS WAF service et de ses AWS ressources, telles que les ACL AWS WAF Web et les groupes de règles.
> Pour plus d'informations sur la protection de vos AWS ressources en utilisant AWS WAF, consultez le reste du AWS WAF guide.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. L'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS WAF, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation ainsi que les lois et réglementations applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS WAF. Les rubriques suivantes expliquent comment procéder à la configuration AWS WAF pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS WAF ressources.

Rubriques

Protection des données dans AWS WAF

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS WAF. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu’Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l’information fédérale).

Nous vous recommandons fortement de ne jamais placer d’informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec AWS WAF ou d'autres Services AWS utilisateurs de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous

saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

AWS WAF les entités, telles que les ACL Web, les groupes de règles et les ensembles d'adresses IP, sont chiffrées au repos, sauf dans certaines régions où le chiffrement n'est pas disponible, notamment en Chine (Pékin) et en Chine (Ningxia). Des clés de chiffrement uniques sont utilisées pour chaque région.

Supprimer des AWS WAF ressources

Vous pouvez supprimer les ressources que vous avez créées dans AWS WAF. Consultez les instructions relatives à chaque type de ressource dans les sections suivantes.

- Supprimer une ACL Web
- Suppression d'un groupe de règles
- Suppression d'un ensemble d'adresses IP
- Suppression d'un ensemble de modèles d'expression régulière

Gestion des identités et des accès pour AWS WAF

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AWS WAF les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Comment AWS WAF fonctionne avec IAM
- Exemples de politiques basées sur l'identité pour AWS WAF
- AWS politiques gérées pour AWS WAF
- Résolution des problèmes AWS WAF d'identité et d'accès

- Utilisation de rôles liés à un service pour AWS WAF

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez. AWS WAF

Utilisateur du service : si vous utilisez le AWS WAF service pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AWS WAF fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS WAF, consultez Résolution des problèmes AWS WAF d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des AWS WAF ressources de votre entreprise, vous avez probablement un accès complet à AWS WAF. C'est à vous de déterminer les AWS WAF fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec AWS WAF, voirComment AWS WAF fonctionne avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à AWS WAF. Pour consulter des exemples de politiques AWS WAF basées sur l'identité que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour AWS WAF

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec

des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en

particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres

personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.

- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les

ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités

figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .

- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS WAF fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS WAF, découvrez les fonctionnalités IAM disponibles. AWS WAF

Fonctionnalités IAM que vous pouvez utiliser avec AWS WAF

Fonction IAM	AWS WAF soutien
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui

Fonction IAM	AWS WAF soutien
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d’identification temporaires	Oui
Transmission des sessions d’accès (FAS)	Oui
Fonctions de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS WAF les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour AWS WAF

Prend en charge les politiques basées sur l’identité	Oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Création de politiques IAM dans le Guide de l’utilisateur IAM.

Avec les politiques IAM basées sur l’identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s’applique à l’utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Pour consulter des exemples de politiques AWS WAF basées sur l'identité, consultez. Exemples de politiques basées sur l’identité pour AWS WAF

Politiques basées sur les ressources au sein de AWS WAF

Prend en charge les politiques basées sur les ressources	Oui

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

AWS WAF utilise des politiques basées sur les ressources pour favoriser le partage de groupes de règles entre les comptes. Vous partagez un groupe de règles que vous possédez avec un autre AWS compte en fournissant les paramètres de politique basés sur les ressources à l'appel d' AWS WAF API `PutPermissionPolicy` ou à un appel de CLI ou de SDK équivalent. Pour plus d'informations, notamment des exemples et des liens vers la documentation des autres langues disponibles, consultez PutPermissionPolicyla référence de l' AWS WAF API. Cette fonctionnalité n'est pas disponible par d'autres moyens, tels que la console ou AWS CloudFormation.

Actions politiques pour AWS WAF

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des AWS WAF actions et des autorisations associées à chacune d'elles, reportez-vous à la section Actions définies par la AWS WAF V2 dans la référence d'autorisation de service.

Les actions de politique en AWS WAF cours utilisent le préfixe suivant avant l'action :

```
wafv2
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "wafv2:action1",
      "wafv2:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes AWS WAF les actions commençant par`List`, incluez l'action suivante :

```
"Action": "wafv2:List*"
```

Pour consulter des exemples de politiques AWS WAF basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour AWS WAF

Actions nécessitant des paramètres d'autorisation supplémentaires

Certaines actions nécessitent des autorisations qui ne peuvent pas être complètement décrites dans la section Actions définies par la AWS WAF version 2 dans la référence d'autorisation de service. Cette section fournit des informations supplémentaires sur les autorisations.

Rubriques

- Autorisations pour AssociateWebACL
- Autorisations pour DisassociateWebACL
- Autorisations pour GetWebACLForResource
- Autorisations pour ListResourcesForWebACL

Autorisations pour **`AssociateWebACL`**

Cette section répertorie les autorisations requises pour associer une ACL Web à une ressource à l'aide de l' AWS WAF action`AssociateWebACL`.

Pour les CloudFront distributions Amazon, utilisez l'action au lieu de cette CloudFront action`UpdateDistribution`. Pour plus d'informations, consultez UpdateDistributionle manuel Amazon CloudFront API Reference.

API REST Amazon API Gateway

Nécessite l'autorisation d'appeler API Gateway `SetWebACL` sur le type de ressource d'API REST et pour appeler AWS WAF `AssociateWebACL` une ACL Web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
```

```
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Application Load Balancer

Nécessite l'autorisation `elasticloadbalancing:SetWebACL` d'appeler une action sur le type de ressource Application Load Balancer et d'appeler une AWS WAF `AssociateWebACL` ACL Web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync API GraphQL

Nécessite l'autorisation d'appeler AWS AppSync `SetWebACL` le type de ressource d'API GraphQL et d'appeler une AWS WAF `AssociateWebACL` ACL Web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
```

```
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Groupe d'utilisateurs Amazon Cognito

Nécessite une autorisation pour appeler l'`AssociateWebACL`action Amazon Cognito sur le type de ressource du groupe d'utilisateurs et pour appeler une AWS WAF `AssociateWebACL` ACL Web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "cognito-idp:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:cognito-idp:*:account-id:userpool/*"
    ]
}
```

AWS App Runner service

Nécessite une autorisation pour appeler l'`AssociateWebACL`action App Runner sur le type de ressource de service App Runner et pour appeler AWS WAF `AssociateWebACL` une ACL Web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
    "Action": [
        "apprunner:AssociateWebAcl"
    ],
    "Resource": [
        "arn:aws:apprunner:*:account-id:service/*/*"
    ]
}
```

AWS Instance d'accès vérifié

Nécessite une autorisation pour appeler l'`ec2:AssociateVerifiedAccessInstanceWebAcl`action sur le type de ressource d'instance Verified Access et pour appeler AWS WAF `AssociateWebACL` une ACL Web.

```
{
    "Sid": "AssociateWebACL1",
    "Effect": "Allow",
    "Action": [
        "wafv2:AssociateWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "AssociateWebACL2",
    "Effect": "Allow",
```

```
    "Action": [
        "ec2:AssociateVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Autorisations pour **`DisassociateWebACL`**

Cette section répertorie les autorisations requises pour dissocier une ACL Web d'une ressource à l'aide de l' AWS WAF action`DisassociateWebACL`.

Pour les CloudFront distributions Amazon, au lieu de cette action, utilisez l' CloudFront action `UpdateDistribution` avec un ID ACL Web vide. Pour plus d'informations, consultez UpdateDistributionle manuel Amazon CloudFront API Reference.

API REST Amazon API Gateway

Nécessite l'autorisation d'appeler API Gateway `SetWebACL` sur le type de ressource d'API REST. Aucune autorisation n'est requise pour appeler AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "apigateway:SetWebACL"
    ],
    "Resource": [
        "arn:aws:apigateway:*::/restapis/*/stages/*"
    ]
}
```

Application Load Balancer

Nécessite l'autorisation d'appeler l'`elasticloadbalancing:SetWebACL`action sur le type de ressource Application Load Balancer. Aucune autorisation n'est requise pour appeler AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
```

```
    "Action": [
        "elasticloadbalancing:SetWebACL"
    ],
    "Resource": [
        "arn:aws:elasticloadbalancing:*:account-id:loadbalancer/app/*/*"
    ]
}
```

AWS AppSync API GraphQL

Nécessite l'autorisation d'appeler AWS AppSync `SetWebACL` le type de ressource de l'API GraphQL. Aucune autorisation n'est requise pour appeler AWS WAF `DisassociateWebACL`.

```
{
    "Sid": "DisassociateWebACL",
    "Effect": "Allow",
    "Action": [
        "appsync:SetWebACL"
    ],
    "Resource": [
        "arn:aws:appsync:*:account-id:apis/*"
    ]
}
```

Groupe d'utilisateurs Amazon Cognito

Nécessite l'autorisation d'appeler l'`DisassociateWebACL`action Amazon Cognito sur le type de ressource du groupe d'utilisateurs et d'appeler. 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 service

Nécessite une autorisation pour appeler l'`DisassociateWebACL`action App Runner sur le type de ressource de service App Runner et pour appeler 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 Instance d'accès vérifié

Nécessite une autorisation pour appeler l'`ec2:DisassociateVerifiedAccessInstanceWebAcl`action sur le type de ressource d'instance Verified Access et pour appeler 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/*"
    ]
}
```

Autorisations pour **`GetWebACLForResource`**

Cette section répertorie les autorisations requises pour obtenir l'ACL Web pour une ressource protégée à l'aide de l' AWS WAF action`GetWebACLForResource`.

Pour les CloudFront distributions Amazon, utilisez l'action au lieu de cette CloudFront action`GetDistributionConfig`. Pour plus d'informations, consultez GetDistributionConfigle manuel Amazon CloudFront API Reference.

> **Note**
>
> `GetWebACLForResource`nécessite l'autorisation d'appeler`GetWebACL`. Dans ce contexte, il `GetWebACL` est AWS WAF utilisé uniquement pour vérifier que votre compte dispose de l'autorisation nécessaire pour accéder à l'ACL Web qui `GetWebACLForResource` renvoie. Lorsque vous appelez`GetWebACLForResource`, un message d'erreur peut s'afficher indiquant que votre compte n'est pas autorisé à effectuer des opérations `wafv2:GetWebACL` sur la ressource. AWS WAF n'ajoute pas ce type d'erreur à l'historique des AWS CloudTrail événements.

API REST Amazon API Gateway, Application Load Balancer et API GraphQL AWS AppSync

Nécessite une autorisation pour appeler AWS WAF `GetWebACLForResource` et `GetWebACL` pour une ACL Web.

```
{
    "Sid": "GetWebACLForResource",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
```

```
    ]
}
```

Groupe d'utilisateurs Amazon Cognito

Nécessite l'autorisation d'appeler l'`GetWebACLForResource`action Amazon Cognito sur le type de ressource du groupe d'utilisateurs et d'appeler AWS WAF `GetWebACLForResource` et. `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 service

Nécessite une autorisation pour appeler l'`DescribeWebAclForService`action App Runner sur le type de ressource de service App Runner et pour appeler AWS WAF `GetWebACLForResource` et`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 Instance d'accès vérifié

Nécessite l'autorisation d'appeler l'`ec2:GetVerifiedAccessInstanceWebAcl`action sur le type de ressource d'instance Verified Access et d'appeler AWS WAF `GetWebACLForResource` et`GetWebACL`.

```
{
    "Sid": "GetWebACLForResource1",
    "Effect": "Allow",
    "Action": [
        "wafv2:GetWebACLForResource",
        "wafv2:GetWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
},
{
    "Sid": "GetWebACLForResource2",
    "Effect": "Allow",
    "Action": [
        "ec2:GetVerifiedAccessInstanceWebAcl"
    ],
    "Resource": [
        "arn:aws:ec2:*:account-id:verified-access-instance/*"
    ]
}
```

Autorisations pour `ListResourcesForWebACL`

Cette section répertorie les autorisations requises pour récupérer la liste des ressources protégées pour une ACL Web à l'aide de l' AWS WAF action`ListResourcesForWebACL`.

Pour les CloudFront distributions Amazon, utilisez l'action au lieu de cette CloudFront action`ListDistributionsByWebACLId`. Pour plus d'informations, consultez ListDistributionsByWebAClid dans le manuel Amazon CloudFront API Reference.

API REST Amazon API Gateway, Application Load Balancer et API GraphQL AWS AppSync

Nécessite une autorisation AWS WAF `ListResourcesForWebACL` pour appeler une ACL Web.

```
{
    "Sid": "ListResourcesForWebACL",
    "Effect": "Allow",
    "Action": [
        "wafv2:ListResourcesForWebACL"
    ],
    "Resource": [
        "arn:aws:wafv2:region:account-id:regional/webacl/*/*"
    ]
}
```

Groupe d'utilisateurs Amazon Cognito

Nécessite l'autorisation d'appeler l'`ListResourcesForWebACL`action Amazon Cognito sur le type de ressource du groupe d'utilisateurs et d'appeler. 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 service

Nécessite une autorisation pour appeler l'`ListAssociatedServicesForWebAcl`action App Runner sur le type de ressource de service App Runner et pour appeler 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 Instance d'accès vérifié

Nécessite une autorisation pour appeler l'`ec2:DescribeVerifiedAccessInstanceWebAclAssociations`action sur le type de ressource d'instance Verified Access et pour appeler 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/*"
    ]
}
```

Ressources politiques pour AWS WAF

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de AWS WAF ressources et leurs ARN, consultez la section Ressources définies par la AWS WAF V2 dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, voir Actions définies par la AWS WAF version 2. Pour autoriser ou refuser l'accès à un sous-ensemble de AWS WAF ressources, incluez l'ARN de la ressource dans l'`resource`élément de votre politique.

Les ARN des AWS WAF `wafv2` ressources ont le format suivant :

```
arn:partition:wafv2:region:account-id:scope/resource-type/resource-name/resource-id
```

Pour obtenir des informations générales sur les spécifications des ARN, consultez Amazon Resource Names (ARN) dans le Référence générale d'Amazon Web Services.

La liste suivante répertorie les exigences spécifiques aux ARN des `wafv2` ressources :

- *`région`* : pour les AWS WAF ressources que vous utilisez pour protéger les CloudFront distributions Amazon, définissez cette option sur`us-east-1`. Sinon, définissez ce paramètre sur la région que vous utilisez avec vos ressources régionales protégées.
- *`portée`* : définissez le champ d'application `global` pour une utilisation avec une CloudFront distribution Amazon ou `regional` pour une utilisation avec l'une des ressources régionales prises AWS WAF en charge. Les ressources régionales sont une API REST Amazon API Gateway, un Application Load Balancer, une API AWS AppSync GraphQL, un groupe d'utilisateurs Amazon Cognito, un AWS App Runner service et une instance Verified Access. AWS
- *`type de ressource`* : Spécifiez l'une des valeurs suivantes :`webacl`,, `rulegroup` `ipsetregexpatternset`, ou. `managedruleset`
- *`resource-name`* : Spécifiez le nom que vous avez donné à la AWS WAF ressource ou spécifiez un caractère générique (*) pour indiquer toutes les ressources qui répondent aux autres spécifications de l'ARN. Vous devez soit spécifier le nom et l'ID de la ressource, soit spécifier un caractère générique pour les deux.
- *`resource-id`* : Spécifiez l'ID de la AWS WAF ressource ou spécifiez un caractère générique (*) pour indiquer toutes les ressources qui répondent aux autres spécifications de l'ARN. Vous devez soit spécifier le nom et l'ID de la ressource, soit spécifier un caractère générique pour les deux.

Par exemple, l'ARN suivante spécifie toutes les listes ACL web avec une portée régionale pour le compte `111122223333` dans la région `us-west-1` :

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

L'ARN suivant spécifie le groupe de règles nommé `MyIPManagementRuleGroup` avec une portée globale pour le compte `111122223333` dans Region `us-east-1` :

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Pour consulter des exemples de politiques AWS WAF basées sur l'identité, consultez. Exemples de politiques basées sur l’identité pour AWS WAF

Clés de conditions de politique pour AWS WAF

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C’est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L’élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu’une instruction est appliquée. L’élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l’aide d’une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l’instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d’espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l’autorisation d’accéder à une ressource uniquement si elle est balisée avec son nom d’utilisateur IAM. Pour plus d’informations, consultez Éléments d’une politique IAM : variables et identifications dans le Guide de l’utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

En outre, AWS WAF prend en charge les clés de condition suivantes que vous pouvez utiliser pour filtrer avec précision vos politiques IAM :

- wafv2 : LogDestinationResource

  Cette clé de condition utilise une spécification Amazon Resource Name (ARN) pour la destination de journalisation. Il s'agit de l'ARN que vous fournissez pour la destination de journalisation lorsque vous utilisez l'appel d'API REST`PutLoggingConfiguration`.

  Vous pouvez spécifier un ARN de manière explicite et vous pouvez spécifier le filtrage de l'ARN. L'exemple suivant indique comment filtrer les ARN des compartiments Amazon S3 dotés d'un emplacement et d'un préfixe spécifiques.

  ```
  "Condition": { "ArnLike": { "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-suffix/custom-prefix/*" } }
  ```

- wafv2 : LogScope

  Cette clé de condition définit la source de la configuration de journalisation dans une chaîne. Actuellement, ce paramètre est toujours défini sur la valeur par défaut de`Customer`, ce qui indique que vous détenez et gérez la destination de journalisation.

Pour voir la liste des clés de AWS WAF condition, voir Clés de condition pour la AWS WAF V2 dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, voir Actions définies par la AWS WAF version 2.

Pour consulter des exemples de politiques AWS WAF basées sur l'identité, consultez. Exemples de politiques basées sur l’identité pour AWS WAF

ACL dans AWS WAF

Prend en charge les listes ACL	Non

Les listes de contrôle d’accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l’autorisation d’accéder à une ressource. Les listes de contrôle d’accès sont similaires aux politiques basées sur les ressources, bien qu’elles n’utilisent pas le format de document de politique JSON.

ABAC avec AWS WAF

Prise en charge d'ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec AWS WAF

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour le service AWS WAF

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Fonctions du service pour AWS WAF

Prend en charge les fonctions du service	Oui

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM.

Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber AWS WAF les fonctionnalités. Modifiez les rôles de service uniquement lorsque AWS WAF vous recevez des instructions à cet effet.

Rôles liés à un service pour AWS WAF

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles AWS WAF liés à un service, consultez. Utilisation de rôles liés à un service pour AWS WAF

Exemples de politiques basées sur l'identité pour AWS WAF

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou modifier les ressources AWS WAF . Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM doit créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS WAF, y compris le format des ARN pour chacun des types de ressources, voir Actions, ressources et clés de condition pour la AWS WAF V2 dans la référence d'autorisation de service.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer AWS WAF des ressources dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez Politiques gérées AWS ou Politiques gérées AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège - Lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès - Vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder

l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles - IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console AWS WAF

Pour accéder à la AWS WAF console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails AWS WAF des ressources de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent utiliser la AWS WAF console, associez également au moins la politique AWS WAF `AWSWAFConsoleReadOnlyAccess` AWS gérée aux entités. Pour plus d'informations sur cette politique gérée, consultezAWS politique gérée : AWSWAFConsoleReadOnlyAccess. Pour plus d'informations sur l'attachement d'une politique gérée à un utilisateur, consultez la section Ajouter des autorisations à un utilisateur dans le guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accordez un accès en lecture seule à AWS WAF, et CloudFront CloudWatch

La politique suivante accorde aux utilisateurs un accès en lecture seule aux AWS WAF ressources, aux distributions CloudFront Web Amazon et aux métriques Amazon CloudWatch . Il est utile pour les utilisateurs qui ont besoin d'une autorisation pour consulter les paramètres AWS WAF des conditions, des règles et des ACL Web afin de voir quelle distribution est associée à une ACL Web et de surveiller les métriques et un échantillon de demandes dans CloudWatch. Ces utilisateurs ne peuvent pas créer, mettre à jour ou supprimer des ressources AWS WAF .

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
         "Action": [
            "wafv2:Get*",
            "wafv2:List*",
            "cloudfront:GetDistribution",
            "cloudfront:GetDistributionConfig",
            "cloudfront:ListDistributions",
            "cloudfront:ListDistributionsByWebACLId",
            "cloudwatch:ListMetrics",
            "cloudwatch:GetMetricStatistics",
            "ec2:DescribeRegions"
         ],
         "Effect": "Allow",
         "Resource": "*"
      }
   ]
}
```

Accordez un accès complet à AWS WAF CloudFront, et CloudWatch

La politique suivante permet aux utilisateurs d'effectuer n'importe quelle AWS WAF opération, d'effectuer n'importe quelle opération sur les distributions CloudFront Web et de surveiller les métriques et un échantillon de demandes introduites CloudWatch. C'est utile pour les utilisateurs AWS WAF administrateurs.

```
{
   "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": "*"
      }
   ]
}
```

Nous vous recommandons vivement de configurer Multi-Factor Authentication (MFA) pour les utilisateurs qui ont des autorisations d'administration. Pour plus d'informations, consultez la section Using Multi-Factor Authentication (MFA) Devices AWS with dans le guide de l'utilisateur IAM.

Accorder l'accès à un single Compte AWS

Cette politique accorde les autorisations suivantes au compte 444455556666 :

- Accès complet à toutes les AWS WAF opérations et ressources.
- Accès en lecture et mise à jour à toutes les CloudFront distributions, ce qui vous permet d'associer des ACL Web et des CloudFront distributions.
- Accès en lecture à toutes les CloudWatch mesures et statistiques des métriques, afin de pouvoir consulter CloudWatch les données et un échantillon de demandes dans la AWS WAF console.

```
{
   "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": [
            "*"
         ]
      }
   ]
}
```

Accorder l'accès à une seule ACL Web

La politique suivante permet aux utilisateurs d'effectuer n'importe quelle AWS WAF opération via la console sur une ACL Web spécifique du compte444455556666.

```
{
    "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": [
                "*"
            ]
        }
    ]
}
```

Accorder l'accès CLI à une ACL Web et à un groupe de règles

La politique suivante permet aux utilisateurs d'effectuer n'importe quelle AWS WAF opération via la CLI sur une ACL Web spécifique et un groupe de règles spécifique dans le compte444455556666.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "wafv2:*"
         ],
         "Resource": [
        "arn:aws:wafv2:us-east-1:444455556666:regional/webacl/
test123/112233d7c-86b2-458b-af83-51c51example",
        "arn:aws:wafv2:us-east-1:444455556666:regional/rulegroup/
test123rulegroup/555555555-6666-1234-abcd-00d11example"
         ]
      }
   ]
}
```

La politique suivante permet aux utilisateurs d'effectuer n'importe quelle AWS WAF opération via la console sur une ACL Web spécifique du compte444455556666.

```
{
    "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 politiques gérées pour AWS WAF

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSWAFReadOnlyAccess

Cette politique accorde des autorisations en lecture seule qui permettent aux utilisateurs d'accéder aux AWS WAF ressources et aux ressources des services intégrés, tels qu'Amazon CloudFront, Amazon API Gateway, Application Load Balancer, AWS AppSync Amazon Cognito et Verified Access. AWS App Runner AWS Vous pouvez associer cette politique à vos identités IAM. AWS WAF associe également cette politique à un rôle de service qui permet AWS WAF d'effectuer des actions en votre nom.

Pour plus de détails sur cette politique, consultez AWSWAFReadOnlyAccessla console IAM.

AWS politique gérée : AWSWAFFullAccess

Cette politique accorde un accès complet aux AWS WAF ressources et aux ressources pour les services intégrés, tels qu'Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito AWS App Runner et Verified Access. AWS Vous pouvez associer cette politique à vos identités IAM. AWS WAF associe également cette politique à un rôle de service qui permet AWS WAF d'effectuer des actions en votre nom.

Pour plus de détails sur cette politique, consultez AWSWAFFullAccessla console IAM.

AWS politique gérée : AWSWAFConsoleReadOnlyAccess

Cette politique accorde des autorisations en lecture seule à la AWS WAF console, qui inclut des ressources pour AWS WAF et pour les services intégrés, tels qu'Amazon CloudFront, Amazon API Gateway, Application Load Balancer, AWS AppSync Amazon Cognito et Verified Access AWS App Runner. AWS Vous pouvez associer cette politique à vos identités IAM. AWS WAF associe également cette politique au rôle de service aiam/home#/policies/arn:aws:iam : :aws:policy/ $ qui permet d'effectuer des actions en votre nom. AWSWAFConsoleFullAccess serviceLevelSummary AWS WAF

Pour plus de détails sur cette politique, consultez AWSWAFConsoleReadOnlyAccessla console IAM.

AWS politique gérée : AWSWAFConsoleFullAccess

Cette politique accorde un accès complet à la AWS WAF console, qui inclut des ressources pour AWS WAF et pour les services intégrés, tels qu'Amazon CloudFront, Amazon API Gateway, Application Load Balancer AWS AppSync, Amazon Cognito AWS App Runner et Verified Access. AWS Vous pouvez associer cette politique à vos identités IAM. AWS WAF associe également cette politique à un rôle de service qui permet AWS WAF d'effectuer des actions en votre nom.

Pour plus de détails sur cette politique, consultez AWSWAFConsoleFullAccessla console IAM.

AWS politique gérée : WAFV2 LoggingServiceRolePolicy

Cette politique permet d' AWS WAF écrire des journaux sur Amazon Data Firehose. Cette politique n'est utilisée que si vous activez la connexion AWS WAF. Cette politique est attachée au rôle lié à un service `AWSServiceRoleForWAFV2Logging`. Pour de plus amples informations sur le rôle lié à un service, veuillez consulter Utilisation de rôles liés à un service pour AWS WAF.

Pour plus de détails sur cette politique, consultez WAFV2 LoggingServiceRolePolicy dans la console IAM.

AWS WAF mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS WAF depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique du AWS WAF document à l'adresseHistorique du document.

Politique	Description du changement	Date
`WAFV2LoggingServiceRolePolicy` Cette politique permet d' AWS WAF écrire des journaux sur Amazon Data Firehose. Il n'est utilisé que si vous activez la journalisation. Détails dans la console IAM : LoggingServiceRolePolicyWAFV2.	Des identifiants de déclaration (SID) ont été ajoutés aux paramètres d'autorisation dans le rôle lié au service auquel cette politique est attachée.	03/06/2024
`AWSServiceRoleForWAFV2Logging` Ce rôle lié à un service fournit des politiques d'autorisation qui permettent d' AWS WAF	Des identifiants de déclaration (SID) ont été ajoutés aux paramètres des autorisations.	03/06/2024

Politique	Description du changement	Date
écrire des journaux sur Amazon Data Firehose. Détails dans la console IAM : AWSServiceRoleForWAFV2Logging.		
AWS WAF ajouts au suivi des modifications	AWS WAF a commencé à suivre les modifications apportées à la politique gérée `WAFV2LoggingServiceRolePolicy` et au rôle lié au service. `AWSServiceRoleForWAFV2Logging`	03/06/2024
`AWSWAFFullAccess` Cette politique permet AWS WAF de gérer les AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFFullAccess.	Autorisations étendues pour ajouter des instances d'accès AWS vérifié aux types de ressources que vous pouvez utiliser pour vous protéger AWS WAF.	17/06/2023
`AWSWAFReadOnlyAccess` Cette politique permet AWS WAF de gérer les AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFReadOnlyAccess.	Autorisations étendues pour ajouter des instances d'accès AWS vérifié aux types de ressources que vous pouvez utiliser pour vous protéger AWS WAF.	17/06/2023

Politique	Description du changement	Date
`AWSWAFConsoleFullAccess` Cette politique permet AWS WAF de gérer les ressources de AWS la console et d'autres AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFConsoleFullAccess.	Autorisations étendues pour ajouter des instances d'accès AWS vérifié aux types de ressources que vous pouvez utiliser pour vous protéger AWS WAF.	17/06/2023
`AWSWAFConsoleReadOnlyAccess` Cette politique permet AWS WAF de gérer les ressources de AWS la console et d'autres AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFConsoleReadOnlyAccess.	Autorisations étendues pour ajouter des instances d'accès AWS vérifié aux types de ressources que vous pouvez utiliser pour vous protéger AWS WAF.	17/06/2023
`AWSWAFFullAccess` Cette politique permet AWS WAF de gérer les AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFFullAccess.	Autorisations étendues pour corriger les paramètres d'accès aux AWS App Runner services.	06/06/2023

Politique	Description du changement	Date
`AWSWAFReadOnlyAccess` Cette politique permet AWS WAF de gérer les AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFReadOnlyAccess.	Autorisations étendues pour corriger les paramètres d'accès aux AWS App Runner services.	06/06/2023
`AWSWAFConsoleFullAccess` Cette politique permet AWS WAF de gérer les ressources de AWS la console et d'autres AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFConsoleFullAccess.	Autorisations étendues pour corriger les paramètres d'accès aux AWS App Runner services.	06/06/2023
`AWSWAFConsoleReadOnlyAccess` Cette politique permet AWS WAF de gérer les ressources de AWS la console et d'autres AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFConsoleReadOnlyAccess.	Autorisations étendues pour corriger les paramètres d'accès aux AWS App Runner services.	06/06/2023

Politique	Description du changement	Date
`AWSWAFFullAccess` Cette politique permet AWS WAF de gérer les AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFFullAccess.	Autorisations étendues pour ajouter AWS App Runner des services aux types de ressources que vous pouvez utiliser pour vous protéger AWS WAF.	30/1
`AWSWAFReadOnlyAccess` Cette politique permet AWS WAF de gérer les AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFReadOnlyAccess.	Autorisations étendues pour ajouter AWS App Runner des services aux types de ressources que vous pouvez utiliser pour vous protéger AWS WAF.	30/1
`AWSWAFConsoleFullAccess` Cette politique permet AWS WAF de gérer les ressources de AWS la console et d'autres AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFConsoleFullAccess.	Autorisations étendues pour ajouter AWS App Runner des services aux types de ressources que vous pouvez utiliser pour vous protéger AWS WAF.	30/1

Politique	Description du changement	Date
`AWSWAFConsoleReadOnlyAccess` Cette politique permet AWS WAF de gérer les ressources de AWS la console et d'autres AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFConsoleReadOnlyAccess.	Autorisations étendues pour ajouter AWS App Runner des services aux types de ressources que vous pouvez utiliser pour vous protéger AWS WAF.	30/1
`AWSWAFFullAccess` Cette politique permet AWS WAF de gérer les AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFFullAccess.	Autorisations étendues pour ajouter des groupes d'utilisateurs Amazon Cognito aux types de ressources que vous pouvez utiliser pour vous protéger. AWS WAF	08-25
`AWSWAFReadOnlyAccess` Cette politique permet AWS WAF de gérer les AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFReadOnlyAccess.	Autorisations étendues pour ajouter des groupes d'utilisateurs Amazon Cognito aux types de ressources que vous pouvez utiliser pour vous protéger. AWS WAF	08-25

Politique	Description du changement	Date
`AWSWAFConsoleFullAccess` Cette politique permet AWS WAF de gérer les ressources de AWS la console et d'autres AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFConsoleFullAccess.	Autorisations étendues pour ajouter des groupes d'utilisateurs Amazon Cognito aux types de ressources que vous pouvez utiliser pour vous protéger. AWS WAF	08-25
`AWSWAFConsoleReadOnlyAccess` Cette politique permet AWS WAF de gérer les ressources de AWS la console et d'autres AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFConsoleReadOnlyAccess.	Autorisations étendues pour ajouter des groupes d'utilisateurs Amazon Cognito aux types de ressources que vous pouvez utiliser pour vous protéger. AWS WAF	08-25

Politique	Description du changement	Date
`AWSWAFFullAccess` Cette politique permet AWS WAF de gérer les AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFFullAccess.	Correction des paramètres d'autorisation pour la livraison des journaux pour Amazon Simple Storage Service (Amazon S3) et Amazon CloudWatch Logs. Cette modification corrige les erreurs de refus d'accès survenues lors de la configuration de la journalisation. Pour plus d'informations sur la journalisation de votre trafic ACL Web, consultezJournalisation AWS WAF du trafic ACL Web.	01/01/11
`AWSWAFConsoleFullAccess` Cette politique permet AWS WAF de gérer les ressources de AWS la console et d'autres AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFConsoleFullAccess.	Correction des paramètres d'autorisation pour la livraison des journaux pour Amazon Simple Storage Service (Amazon S3) et Amazon CloudWatch Logs. Cette modification corrige les erreurs d'accès survenues lors de la configuration de la journalisation. Pour plus d'informations sur la journalisation de votre trafic ACL Web, consultez Journalisation AWS WAF du trafic ACL Web.	01/01/11

Politique	Description du changement	Date
`AWSWAFFullAccess` Cette politique permet AWS WAF de gérer les AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFFullAccess.	Ajout de nouvelles autorisations pour des options de journalisation étendues. Cette modification donne AWS WAF accès aux destinations de journalisation supplémentaires Amazon Simple Storage Service (Amazon S3) et Amazon CloudWatch Logs. Pour plus d'informations sur la journalisation de votre trafic ACL Web, consultezJournalisation AWS WAF du trafic ACL Web.	2021-11-15
`AWSWAFConsoleFullAccess` Cette politique permet AWS WAF de gérer les ressources de AWS la console et d'autres AWS ressources en votre nom dans AWS WAF et dans les services intégrés. Détails dans la console IAM : AWSWAFConsoleFullAccess.	Ajout de nouvelles autorisations pour des options de journalisation étendues. Cette modification donne AWS WAF accès aux destinations de journalisation supplémentaires Amazon Simple Storage Service (Amazon S3) et Amazon CloudWatch Logs. Pour plus d'informations sur la journalisation de votre trafic ACL Web, consultezJournalisation AWS WAF du trafic ACL Web.	2021-11-15

Politique	Description du changement	Date
AWS WAF a commencé à suivre les modifications	AWS WAF a commencé à suivre les modifications apportées AWS à ses politiques gérées.	01-03-2021

Résolution des problèmes AWS WAF d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS WAF IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS WAF
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS WAF ressources

Je ne suis pas autorisé à effectuer une action dans AWS WAF

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `wafv2:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wafv2:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `wafv2:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à AWS WAF.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans AWS WAF. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS WAF ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS WAF en charge, consultezComment AWS WAF fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.

- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour connaître la différence entre l'utilisation de rôles et de politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Utilisation de rôles liés à un service pour AWS WAF

AWS WAF utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à. AWS WAF Les rôles liés au service sont prédéfinis par AWS WAF et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration AWS WAF car vous n'avez pas à ajouter manuellement les autorisations nécessaires. AWS WAF définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS WAF peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisations. Cette politique d'autorisations ne peut pas être attachée à une autre entité IAM.

Vous ne pouvez supprimer un rôle lié à un service qu'après avoir supprimé les ressources connexes du rôle. Cela protège vos AWS WAF ressources car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour AWS WAF

AWS WAF utilise le rôle lié au service `AWSServiceRoleForWAFV2Logging` pour écrire des journaux dans Amazon Data Firehose. Ce rôle n'est utilisé que si vous activez la connexion AWS WAF. Pour de plus amples informations sur la journalisation, veuillez consulter Journalisation AWS WAF du trafic ACL Web.

Ce rôle lié au service est attaché à la politique AWS gérée. `WAFV2LoggingServiceRolePolicy` Pour plus d'informations sur la stratégie gérée, consultez AWS politique gérée : WAFV2 LoggingServiceRolePolicy.

Le rôle lié à un service `AWSServiceRoleForWAFV2Logging` fait confiance au service `wafv2.amazonaws.com` pour endosser le rôle.

Les politiques d'autorisation du rôle permettent AWS WAF d'effectuer les actions suivantes sur les ressources spécifiées :

- Actions Amazon Data Firehose : `PutRecord` et sur les ressources de flux de données `PutRecordBatch` Firehose dont le nom commence par. `aws-waf-logs-` Par exemple, `aws-waf-logs-us-east-2-analytics`.
- AWS Organizations action : `DescribeOrganization` sur les ressources des organisations.

Voir le rôle complet lié au service dans la console IAM :. AWSServiceRoleForWAFV2Logging

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Création d'un rôle lié à un service pour AWS WAF

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez la AWS WAF connexion au AWS Management Console, ou que vous faites une `PutLoggingConfiguration` demande dans la AWS WAF CLI ou l' AWS WAF API, le rôle lié au service est AWS WAF créé pour vous.

Vous devez disposez de l'autorisation `iam:CreateServiceLinkedRole` pour activer la journalisation.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous activez la AWS WAF journalisation, le rôle lié au service est à nouveau AWS WAF créé pour vous.

Modification d'un rôle lié à un service pour AWS WAF

AWS WAF ne vous permet pas de modifier le rôle `AWSServiceRoleForWAFV2Logging` lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom

du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Editing a Service-Linked Role (Modification d'un rôle lié à un service) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour AWS WAF

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le AWS WAF service utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer AWS WAF les ressources utilisées par **`AWSServiceRoleForWAFV2Logging`**

1. Sur la AWS WAF console, supprimez la journalisation de chaque ACL Web. Pour plus d'informations, consultez Journalisation AWS WAF du trafic ACL Web.
2. Au moyen de l'API ou de l'interface de ligne de commande, envoyez une requête `DeleteLoggingConfiguration` pour chaque liste ACL web avec la journalisation activée. Pour plus d'informations, veuillez consulter AWS WAF Référence d'API .

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, l'interface de ligne de commande IAM ou l'API IAM pour supprimer le rôle lié à un service `AWSServiceRoleForWAFV2Logging`. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service AWS WAF

AWS WAF prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez Points de terminaison et quotas AWS WAF.

Connexion et surveillance AWS WAF

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité AWS WAF et des performances de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. AWS fournit plusieurs outils pour surveiller vos AWS WAF ressources et répondre à des événements potentiels :

CloudWatch Alarmes Amazon

À l'aide d' CloudWatch alarmes, vous observez une seule métrique sur une période que vous spécifiez. Si la métrique dépasse un seuil donné, CloudWatch envoie une notification à une rubrique ou AWS Auto Scaling à une politique Amazon SNS. Pour plus d’informations, consultez Surveillance avec Amazon CloudWatch.

AWS CloudTrail journaux

CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS WAF. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS WAF, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires. Pour plus d’informations, consultez Journalisation des appels d'API AWS CloudTrail avec.

AWS WAF journalisation du trafic ACL Web

AWS WAF propose la journalisation du trafic analysé par vos ACL Web. Les journaux incluent des informations telles que l'heure à laquelle la demande AWS WAF a été reçue de votre AWS ressource protégée, des informations détaillées sur la demande et le paramètre d'action pour la règle à laquelle la demande correspond. Pour plus d'informations, voir Journalisation AWS WAF du trafic ACL Web.

Validation de conformité pour AWS WAF

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.

- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS WAF

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l’infrastructure dans AWS WAF

En tant que service géré, AWS WAF il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder AWS WAF via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l’aide d’un ID de clé d’accès et d’une clé d’accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d’identification de sécurité temporaires et signer les demandes.

AWS WAF quotas

> **Note**
>
> Il s'agit de la dernière version de AWS WAF. Pour AWS WAF Classic, voirAWS WAF classique.

AWS WAF est soumis aux quotas suivants (anciennement appelés limites). Ces quotas sont les mêmes pour toutes les régions dans lesquelles AWS WAF il est disponible. Chaque région est soumise à ces quotas individuellement. Les quotas ne sont pas cumulés entre les différentes régions.

AWS WAF a des quotas par défaut sur le nombre maximum d'entités que vous pouvez avoir par compte. Vous pouvez demander une augmentation de ces quotas.

Ressource	Quota par défaut par compte et par région
Nombre maximum d'ACL Web	100
Nombre maximum de groupes de règles	100
Nombre maximum d'ensembles d'adresses IP	100
Nombre maximum de demandes par seconde par ACL Web	25 000
Nombre maximum d'en-têtes de demande personnalisés par ACL Web ou groupe de règles	100
Nombre maximum d'en-têtes de réponse personnalisés par ACL Web ou groupe de règles	100
Nombre maximum de corps de réponse personnalisés par ACL Web ou groupe de règles	50
Nombre maximum de domaines de jetons dans une liste de domaines de jetons ACL Web	10

Le nombre maximum de demandes par seconde (RPS) autorisé CloudFront est défini CloudFront et décrit dans le Guide du CloudFront développeur. AWS WAF

AWS WAF a fixé des quotas sur les paramètres d'entité suivants par compte et par région. Ces quotas ne peuvent pas être modifiés.

Ressource	Quota par compte et par région
Unités de capacité ACL Web (WCU) maximales par ACL Web*	5 000
Nombre maximum de WCU par groupe de règles	5 000
Nombre maximum d'instructions de référence par groupe de règles. Dans un groupe de règles, une instruction de référence peut faire référence à un ensemble d'adresses IP ou à un ensemble de modèles regex.	50
Nombre maximum d'instructions de référence par ACL Web. Dans une ACL Web, une instruction de référence peut faire référence à un groupe de règles, à un ensemble d'adresses IP ou à un ensemble de modèles regex.	50
Nombre maximum d'adresses IP en notation CIDR par ensemble d'adresses IP	10 000
Nombre maximum de règles basées sur le taux par ACL Web	10
Nombre maximum de règles basées sur le taux par groupe de règles	4
Fréquence de demande minimum pouvant être défini pour une règle basée sur la fréquence	100
Nombre maximum d'adresses IP uniques pouvant être limitées par règle basée sur le débit	10 000
Nombre maximal de caractères dans une instruction de correspondance de chaîne	200
Nombre maximum de caractères dans chaque modèle d'expression régulière	200

Ressource	Quota par compte et par région
Nombre maximum de modèles de regex uniques par ensemble de regex	10
Nombre maximum d'ensembles de regex	10
Taille maximale du corps d'une requête Web pouvant être inspecté pour détecter la présence d'Application Load Balancer et de ses protections AWS AppSync	8 Ko
Taille maximale du corps d'une requête Web pouvant être inspectée pour détecter les protections CloudFront API Gateway, Amazon Cognito, App Runner et Verified Access**	64 Ko
Nombre maximal de transformations de texte par instruction de règle	10
Taille maximale du contenu du corps de réponse personnalisée pour une seule définition de réponse personnalisée	4 Ko
Nombre maximum d'en-têtes personnalisés pour une seule définition de réponse personnalisée	10
Nombre maximum d'en-têtes personnalisés pour une seule définition de demande personnalisée	10
Taille combinée maximale de tout le contenu du corps de réponse pour un seul groupe de règles ou une seule ACL Web	50 Ko

*L'utilisation de plus de 1 500 WCU dans une ACL Web entraîne des coûts supérieurs au prix de base de l'ACL Web. Pour plus d'informations, veuillez consulter les sections AWS WAF unités de capacité ACL Web (WCU) et Tarification d'AWS WAF.

**Par défaut, la limite d'inspection corporelle est fixée à 16 Ko pour les CloudFront ressources API Gateway, Amazon Cognito, App Runner et Verified Access, mais vous pouvez l'augmenter pour n'importe laquelle de ces ressources dans votre configuration ACL Web, jusqu'au maximum indiqué. Pour plus d’informations, consultez Gestion des limites de taille des organismes inspectés.

AWS WAF dispose des quotas fixes d'appels suivants par compte et par région. Ces quotas s'appliquent au total des appels au service par tous les moyens disponibles, y compris la console, l'interface de ligne de commande, AWS CloudFormation, l'API REST et les kits SDK. Ces quotas ne peuvent pas être modifiés.

Type d'appel	Quota par compte et par région
Nombre maximal d'appels à `AssociateWebACL`	Une demande toutes les 2 secondes
Nombre maximal d'appels à `DisassociateWebACL`	Une demande toutes les 2 secondes
Nombre maximal d'appels à `GetWebACLForResource`	Une demande par seconde
Nombre maximal d'appels à `ListResourcesForWebACL`	Une demande par seconde
Nombre maximal d'appels à toute action `Get` ou `List` individuelle, si aucun autre quota n'est défini pour elle	Cinq demandes par seconde
Nombre maximal d'appels à toute action `Create`, `Put` ou `Update` individuelle, si aucun autre quota n'est défini pour elle	Une demande par seconde

Migration de vos ressources AWS WAF classiques vers AWS WAF

Cette section fournit des conseils pour migrer vos règles et vos ACL Web de AWS WAF Classic vers. AWS WAF AWS WAF est sorti en novembre 2019. Si vous avez créé des ressources telles que des règles et des ACL Web à l'aide de AWS WAF Classic, vous devez soit les utiliser à l'aide de AWS WAF Classic, soit les migrer vers cette dernière version.

Avant de commencer votre travail de migration, familiarisez-vous avec le tout AWS WAF en lisant ce qui suitAWS WAF.

Rubriques

Pourquoi migrer vers AWS WAF ?

La dernière version de AWS WAF apporte de nombreuses améliorations par rapport à la version précédente, tout en conservant la plupart des concepts et de la terminologie auxquels vous êtes habitué.

La liste suivante décrit les principales modifications apportées à la dernière version d' AWS WAF. Avant de poursuivre votre migration, veuillez prendre le temps de consulter cette liste et de vous familiariser avec le reste du AWS WAF guide.

- AWS Règles gérées pour AWS WAF : les groupes de règles désormais disponibles via AWS Managed Rules offrent une protection contre les menaces Web courantes. La plupart de ces groupes de règles sont inclus gratuitement dans AWS WAF. Pour plus d'informations, consultez AWS Liste des groupes de règles gérées et le billet de blog Annunding AWS Managed Rules for AWS WAF.
- Nouvelle AWS WAF API — La nouvelle API vous permet de configurer toutes vos AWS WAF ressources à l'aide d'un seul ensemble d'API. Pour distinguer les applications régionales et globales, la nouvelle API inclut un paramètre `scope`. Pour plus d'informations sur l'API, consultez les actions AWS WAFV2 et les types de données AWS WAFV2.

  Dans les API, les SDK, les CLI et AWS CloudFormation AWS WAF Classic conserve ses schémas de dénomination et cette dernière version de AWS WAF est désignée par un `V2` ou`v2`, selon le contexte.
- Quotas de service simplifiés (limites) : autorise AWS WAF désormais un plus grand nombre de règles par ACL Web et vous permet d'exprimer des modèles de regex plus longs. Pour plus d'informations, consultez AWS WAF quotas.
- Les limites des ACL Web sont désormais basées sur les besoins informatiques. Les limites des ACL Web sont désormais basées sur les unités de capacité des ACL Web (WCU). AWS WAF calcule le WCU d'une règle en fonction de la capacité opérationnelle requise pour exécuter la règle.

La WCU d'une ACL Web est la somme de la WCU de toutes les règles et de tous les groupes de règles de l'ACL Web.

Pour des informations générales sur la WCU, consultezComment AWS WAF fonctionne. Pour plus d'informations sur l'utilisation de la WCU par chaque règle, consultezNotions de base sur les énoncés.

- Rédaction de règles basée sur des documents : vous pouvez désormais écrire et exprimer des règles, des groupes de règles et des ACL Web au format JSON. Vous n'avez plus besoin d'utiliser des appels d'API individuels pour créer des conditions différentes, puis associer les conditions à une règle. Cela simplifie grandement la façon dont vous écrivez et maintenez votre code. Vous pouvez accéder à un format JSON de vos listes ACL web via la console lorsque vous affichez la liste ACL web, en choisissant Télécharger une liste ACL web en tant que JSON. Lorsque vous créez votre propre règle, vous pouvez accéder à sa représentation JSON en choisissant l'éditeur JSON de règle.
- Imbrication des règles et prise en charge complète des opérations logiques : vous pouvez écrire des règles combinées complexes en utilisant des instructions de règles logiques et en utilisant l'imbrication. Vous pouvez créer des instructions, telles que `[A AND NOT(B OR C)]`. Pour plus d'informations, consultez Déclarations de règles logiques.
- Règles basées sur les taux améliorées : dans la dernière version de AWS WAF, vous pouvez personnaliser la fenêtre temporelle évaluée par la règle et la manière dont la règle agrège les demandes. Vous pouvez personnaliser l'agrégation en combinant un certain nombre de caractéristiques de requêtes Web. De plus, les dernières règles basées sur les tarifs réagissent plus rapidement aux variations du trafic. Pour plus d'informations, consultez Instruction de règle basée sur un taux.
- Prise en charge de plages CIDR variables pour les ensembles d'adresses IP — Les spécifications des ensembles d'adresses IP offrent désormais une plus grande flexibilité dans les plages d'adresses IP. Pour IPv4, AWS WAF prend en charge`/1`. `/32` Pour IPv6, AWS WAF prend `/1` en charge`/128`. Pour de plus amples informations sur les ensembles d'adresses IP, veuillez consulter Instruction de correspondance d'ensemble d'adresses IP de règle.
- Transformations de texte chaînables : possibilité d' AWS WAF effectuer plusieurs transformations de texte sur le contenu d'une requête Web avant de l'inspecter. Pour plus d'informations, consultez Options de transformation du texte.
- Expérience de console améliorée — La nouvelle AWS WAF console intègre un générateur de règles visuel et une conception de console plus intuitive pour l'utilisateur.

- Options étendues pour les AWS WAF politiques de Firewall Manager : dans le cadre de la gestion des ACL AWS WAF Web par Firewall Manager, vous pouvez désormais créer un ensemble de groupes de règles qui AWS WAF traitent en premier et un ensemble de groupes de règles qui AWS WAF traitent en dernier. Après avoir appliqué la AWS WAF politique, les propriétaires de comptes locaux peuvent ajouter leurs propres groupes de règles qui AWS WAF traitent entre ces deux ensembles. Pour plus d'informations sur les AWS WAF politiques de Firewall Manager, consultezAWS WAF politiques.
- AWS CloudFormation prise en charge de tous les types d'instructions de règles : AWS WAF in AWS CloudFormation prend en charge tous les types d'instructions de règles pris en charge par la AWS WAF console et l'API. En outre, vous pouvez facilement convertir les règles que vous écrivez en format JSON au format YAML.

Fonctionnement de la migration

La migration automatisée prend en charge la majeure partie de votre configuration ACL Web AWS WAF classique, vous laissant quelques tâches à gérer manuellement.

Voici les étapes de haut niveau pour la migration d'une liste ACL web.

1. La migration automatique lit tout ce qui concerne votre ACL Web existante, sans rien modifier ni supprimer dans AWS WAF Classic. Il crée une représentation de l'ACL Web et de ses ressources associées, compatible avec AWS WAF. Il génère un AWS CloudFormation modèle pour la nouvelle ACL Web et le stocke dans un compartiment Amazon S3.
2. Vous déployez le modèle dans AWS CloudFormation, afin de recréer l'ACL Web et les ressources associées dans AWS WAF.
3. Vous examinez la liste ACL web et effectuez manuellement la migration, en vous assurant que votre nouvelle liste ACL web profite pleinement des fonctionnalités de la dernière version d' AWS WAF.
4. Vous basculez manuellement vos ressources protégées vers la nouvelle liste ACL web.

Mises en garde et limites concernant la migration

La migration ne prend pas en compte tous vos paramètres, tels qu'ils sont définis dans AWS WAF Classic. Quelques éléments, tels que les règles gérées, ne correspondent pas exactement entre les deux versions. D'autres paramètres, tels que les associations de l'ACL Web avec AWS des

ressources protégées, sont initialement désactivés dans la nouvelle version afin que vous puissiez les ajouter lorsque vous êtes prêt.

La liste suivante décrit les mises en garde concernant la migration et les étapes à suivre pour y répondre. Utilisez cette présentation pour planifier votre migration. Plus tard, les étapes détaillées de la migration vous expliquent les étapes d'atténuation recommandées.

- Compte unique : vous ne pouvez migrer les ressources AWS WAF classiques d'un compte que vers les AWS WAF ressources du même compte.
- Règles gérées : la migration n'inclut aucune règle gérée par les AWS Marketplace vendeurs. Certains AWS Marketplace vendeurs disposent de règles gérées équivalentes AWS WAF auxquelles vous pouvez vous abonner à nouveau. Avant cela, passez en revue les règles AWS gérées fournies avec la dernière version de AWS WAF. La plupart d'entre eux sont gratuits pour les AWS WAF utilisateurs. Pour de plus amples informations sur les règles gérées, veuillez consulter Groupes de règles gérés.
- Associations ACL Web : la migration ne crée aucune association entre l'ACL Web et les ressources protégées. Ce comportement est intégré à la conception pour éviter d'affecter votre charge de travail de production. Après avoir vérifié que tout a été correctement migré, associez la nouvelle liste ACL web à vos ressources.
- Journalisation : la journalisation de l'ACL Web migrée est désactivée par défaut. Ce comportement est intégré à la conception. Activez la journalisation lorsque vous êtes prêt à passer de la AWS WAF version classique à AWS WAF.
- AWS Firewall Manager groupes de règles : la migration ne gère pas les groupes de règles gérés par Firewall Manager. Vous pouvez migrer une ACL Web gérée par Firewall Manager, mais la migration n'implique pas le groupe de règles. Au lieu d'utiliser l'outil de migration pour ces ACL Web, recréez la politique pour les nouvelles AWS WAF dans Firewall Manager.

  > **Note**
  >
  > Les groupes de règles gérés par Firewall Manager pour AWS WAF Classic étaient les groupes de règles Firewall Manager. Dans la nouvelle version de AWS WAF, les groupes de règles sont des groupes de AWS WAF règles. Fonctionnellement, ils sont identiques.

- AWS WAF Automatisations de sécurité — N'essayez pas de migrer des automatisations AWS WAF de sécurité. La migration ne convertit pas les fonctions Lambda, qui pourraient être utilisées par les automatisations. Lorsqu'une nouvelle solution d'automatisation de AWS WAF sécurité compatible avec la dernière version est disponible AWS WAF, redéployez-la.

Migration d'une ACL Web de AWS WAF Classic vers AWS WAF

Pour migrer une liste ACL web et basculer vers elle, effectuez la migration automatisée, puis exécutez une série d'étapes manuelles.

Rubriques

Migration d'une liste ACL web : migration automatisée

Pour migrer automatiquement une configuration ACL Web de AWS WAF Classic vers AWS WAF

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Choisissez Basculer vers la AWS WAF version classique et passez en revue vos paramètres de configuration pour l'ACL Web. Notez les paramètres en tenant compte des mises en garde et des limites décrites dans la section précédente, Mises en garde et limites concernant la migration.
3. Dans le dialogue d'information en haut, recherchez la phrase commençant par Migrate Web ACL et choisissez le lien vers l'assistant de migration. Cette opération lance l'assistant de migration.

   Si la boîte de dialogue d'information ne s'affiche pas, vous l'avez peut-être fermée depuis le lancement de la console AWS WAF Classic. Dans la barre de navigation, choisissez Basculer vers le nouveau, AWS WAF puis sélectionnez Basculer vers le mode AWS WAF classique, et le dialogue d'information devrait réapparaître.
4. Sélectionnez la liste ACL web à migrer.
5. Pour la configuration de la migration, fournissez un compartiment Amazon S3 à utiliser pour le modèle. Vous avez besoin d'un compartiment Amazon S3 correctement configuré pour l'API de migration afin de stocker le AWS CloudFormation modèle généré.

   - Si le compartiment est chiffré, le chiffrement doit utiliser les clés Amazon S3 (SSE-S3). La migration ne prend pas en charge le chiffrement avec des AWS Key Management Service clés (SSE-KMS).

- Le nom du compartiment doit commencer par `aws-waf-migration-`. Par exemple, `aws-waf-migration-my-web-acl`.
- Le compartiment doit se trouver dans la région où vous déployez le modèle. Par exemple, pour une ACL Web dans`us-west-2`, vous devez utiliser un compartiment Amazon S3 dans `us-west-2` lequel vous devez déployer la pile de modèles`us-west-2`.

6. Pour la stratégie de compartiment S3, nous vous recommandons de choisir Appliquer automatiquement la stratégie de compartiment requise pour la migration. Sinon, si vous souhaitez gérer le compartiment par vous-même, vous devez appliquer manuellement la stratégie de compartiment suivante :

   - Pour les CloudFront applications Amazon mondiales (`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>/
*"
        }
    ]
}
```

   - Pour les applications Amazon API Gateway ou Application Load Balancer régionales () `waf-regional` :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "apiv2migration.waf-regional.amazonaws.com"
            },
            "Action": "s3:PutObject",
```

```
            "Resource": "arn:aws:s3:::<BUCKET_NAME>/AWSWAF/<CUSTOMER_ACCOUNT_ID>/
*"
        }
    ]
}
```

7. Pour Choisir comment gérer les règles qui ne peuvent pas être migrées, choisissez d'exclure les règles qui ne peuvent pas être migrées ou d'arrêter la migration. Pour de plus amples informations sur les règles qui ne peuvent pas être migrées, veuillez consulter Mises en garde et limites concernant la migration.
8. Choisissez Suivant.
9. Pour Créer un AWS CloudFormation modèle, vérifiez vos paramètres, puis choisissez Commencer à créer un AWS CloudFormation modèle pour démarrer le processus de migration. Cela peut prendre quelques minutes selon la complexité de votre liste ACL web.
10. Dans Créer et exécuter une AWS CloudFormation pile pour terminer la migration, vous pouvez choisir d'accéder à la AWS CloudFormation console pour créer une pile à partir du modèle, afin de créer la nouvelle ACL Web et ses ressources. Pour ce faire, choisissez Create AWS CloudFormation stack.

Une fois le processus de migration automatique terminé, vous êtes prêt à passer aux étapes de suivi manuel. veuillez consulter Migration d'une liste ACL web : suivi manuel.

Migration d'une liste ACL web : suivi manuel

Une fois la migration automatisée terminée, examinez la liste ACL web nouvellement créée et remplissez les composants que la migration n'entraîne pas. La procédure suivante couvre les aspects de la gestion de la liste ACL web qui ne sont pas gérés par la migration. Pour la liste, veuillez consulter Mises en garde et limites concernant la migration.

Pour terminer la migration de base - étapes manuelles

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. La console doit automatiquement utiliser la dernière version de AWS WAF. Pour vérifier cela, dans le volet de navigation, vérifiez que l'option Passer en mode AWS WAF classique est visible. Si vous voyez Passer à la nouvelle version AWS WAF, choisissez-la pour passer à la dernière version.
3. Dans le volet de navigation, choisissez Web ACLs.

4. Sur la page Listes ACL web, recherchez votre nouvelle liste ACL web dans la liste de la région dans laquelle vous l'avez créée. Choisissez le nom de la liste ACL web pour afficher les paramètres de la liste ACL web.
5. Vérifiez tous les paramètres de la nouvelle ACL Web par rapport à votre ancienne ACL Web AWS WAF classique. Par défaut, la journalisation et les associations de ressources protégées sont désactivées. Vous les activez lorsque vous êtes prêt à basculer.
6. Si votre ACL Web AWS WAF classique comportait une règle basée sur le taux assortie d'une condition, celle-ci n'a pas été prise en compte lors de la migration. Vous pouvez ajouter des conditions à la règle dans la nouvelle liste ACL web.

   a. Sur la page des paramètres de la liste ACL web, sélectionnez l'onglet Règles.

   b. Dans la liste, recherchez votre règle basée sur le débit, sélectionnez-la et choisissez Modifier.

   c. Pour Critères pour comptabiliser les demandes dans la limite de débit, sélectionnez Ne prendre en compte que les demandes correspondant aux critères d'une instruction de règle, puis indiquez vos critères supplémentaires. Vous pouvez ajouter les critères à l'aide de n'importe quelle instruction de règle pouvant être imbriquée, y compris des instructions logiques. Pour de plus amples informations sur vos choix, veuillez consulter Instruction de règle basée sur un taux.
7. Si votre ACL Web AWS WAF classique comportait un groupe de règles géré, l'inclusion du groupe de règles n'a pas été prise en compte lors de la migration. Vous pouvez ajouter des groupes de règles gérées à la nouvelle liste ACL web. Consultez les informations relatives aux groupes de règles gérés, notamment la liste des règles AWS gérées disponibles avec la nouvelle version de AWS WAF, à l'adresseGroupes de règles gérés. Pour ajouter un groupe de règles gérées, procédez comme suit :

   a. Dans la page des paramètres de la liste ACL web, choisissez l'onglet Règles de la liste ACL web.

   b. Choisissez Ajouter des règles, puis Ajouter des groupes de règles gérées.

   c. Développez la liste pour le fournisseur de votre choix et sélectionnez les groupes de règles que vous souhaitez ajouter. Pour AWS Marketplace les vendeurs, vous devrez peut-être vous abonner aux groupes de règles. Pour de plus amples informations sur l'utilisation de groupes de règles gérées dans votre liste ACL web, veuillez consulter Groupes de règles gérés et Évaluation des règles ACL Web et des groupes de règles.

Une fois le processus de migration de base terminé, nous vous recommandons d'examiner vos besoins et d'envisager d'autres options, afin de vous assurer que la nouvelle configuration est aussi efficace que possible et qu'elle utilise les dernières options de sécurité disponibles. veuillez consulter Migration d'une liste ACL web : considérations supplémentaires.

Migration d'une liste ACL web : considérations supplémentaires

Passez en revue votre nouvelle ACL Web et considérez les options qui s'offrent AWS WAF à vous dans la nouvelle pour vous assurer que la configuration est aussi efficace que possible et qu'elle utilise les dernières options de sécurité disponibles.

Règles AWS gérées supplémentaires

Envisagez d'implémenter des règles AWS gérées supplémentaires dans votre ACL Web afin d'améliorer le niveau de sécurité de votre application. Ils sont inclus sans AWS WAF frais supplémentaires. AWS Les règles gérées comportent les types de groupes de règles suivants :

- Les groupes de règles de base fournissent une protection générale contre une variété de menaces courantes, telles que l'arrêt de l'intégration des entrées erronées connues à votre application et l'interdiction d'accès à la page d'administration.
- Les groupes de règles spécifiques au cas d'utilisation offrent une protection incrémentielle pour de nombreux cas d'utilisation et environnements.
- Les listes de réputation d'adresses IP fournissent des informations sur les menaces basées sur l'adresse IP source du client.

Pour plus d’informations, consultez AWS Règles gérées pour AWS WAF.

Optimisation et nettoyage des règles

Réexaminez vos anciennes règles et optimisez-les en les réécrivant ou en supprimant celles qui sont obsolètes. Par exemple, si par le passé, vous avez déployé un AWS CloudFormation modèle tiré du document technique intitulé « Les 10 principales vulnérabilités des applications Web de l'OWASP », « Prepare for the OWASP Top 10 Web Application Vulnerabilities Using » AWS WAF et de notre nouveau livre blanc, vous devriez envisager de le remplacer par des règles gérées. AWS Bien que le concept décrit dans le document soit toujours applicable et puisse vous aider à rédiger vos propres règles, les règles créées par le modèle ont été largement remplacées par les règles AWS gérées.

CloudWatch Mesures et alarmes Amazon

Revoyez vos CloudWatch statistiques Amazon et configurez des alarmes selon vos besoins. La migration n'entraîne pas d'CloudWatch alarmes et il est possible que les noms de vos métriques ne correspondent pas à vos attentes.

Examen avec votre équipe d'application

Collaborez avec votre équipe d'application et vérifiez votre niveau de sécurité. Découvrez quels champs sont analysés fréquemment par l'application et ajoutez des règles pour nettoyer l'entrée en conséquence. Recherchez les cas périphériques et ajoutez des règles pour intercepter ces cas si la logique métier de l'application ne les traite pas.

Planification du basculement

Planifiez le calendrier du commutateur avec votre équipe d'application. Le passage de l'ancienne association ACL Web à la nouvelle peut prendre un peu de temps pour se propager à toutes les zones où vos ressources sont stockées. Le temps de propagation peut aller de quelques secondes à plusieurs minutes. Pendant ce temps, certaines demandes seront traitées par l'ancienne ACL Web et d'autres par la nouvelle ACL Web. Vos ressources seront protégées tout au long du changement, mais il est possible que vous remarquiez des incohérences dans le traitement des demandes pendant le changement.

Lorsque vous êtes prêt à basculer, suivez la procédure dans Migration d'une liste ACL web : basculement.

Migration d'une liste ACL web : basculement

Après avoir vérifié vos nouveaux paramètres ACL Web, vous pouvez commencer à les utiliser à la place de votre ACL Web AWS WAF classique.

Pour commencer à utiliser votre nouvelle ACL AWS WAF Web

1. Associez l'ACL AWS WAF Web aux ressources que vous souhaitez protéger, en suivant les instructions deAssocier ou dissocier une ACL Web à une ressource AWS. Cela dissocie automatiquement les ressources de l'ancienne liste ACL web.

   La propagation du commutateur peut prendre de quelques secondes à plusieurs minutes. Pendant ce temps, certaines demandes peuvent être traitées par l'ancienne ACL Web et d'autres par la nouvelle ACL Web. Vos ressources seront protégées tout au long du changement, mais vous remarquerez peut-être des incohérences dans le traitement des demandes jusqu'à ce qu'elles soient terminées.

2. Configurez la journalisation pour la nouvelle liste ACL web, en suivant les instructions dans Journalisation AWS WAF du trafic ACL Web.
3. (Facultatif) Si votre ACL Web AWS WAF classique n'est plus associée à aucune ressource, envisagez de la supprimer complètement de AWS WAF Classic. Pour plus d’informations, consultez Suppression d'une liste ACL web.

AWS WAF classique

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

AWS WAF Classic est un pare-feu d'applications Web qui vous permet de surveiller les requêtes HTTP et HTTPS qui sont transmises à une API Amazon API Gateway, à Amazon CloudFront ou à un Application Load Balancer. AWS WAF Classic vous permet également de contrôler l'accès à votre contenu. Selon les conditions que vous spécifiez, telles que les adresses IP d'où proviennent les demandes ou les valeurs des chaînes de requête, API Gateway CloudFront ou un Application Load Balancer répond aux demandes soit avec le contenu demandé, soit avec un code d'état HTTP 403 (Forbidden). Vous pouvez également configurer CloudFront pour renvoyer une page d'erreur personnalisée lorsqu'une demande est bloquée.

Rubriques

- AWS WAF Quotas classiques

Configuration de AWS WAF Classic

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Cette rubrique décrit les étapes préliminaires, telles que la création d'un compte utilisateur, pour vous préparer à utiliser AWS WAF Classic. Ils ne vous sont pas facturés. Seuls les AWS services que vous utilisez vous sont facturés.

> **Note**
>
> Si vous êtes un nouvel utilisateur AWS WAF, ne suivez pas ces étapes de configuration pour AWS WAF Classic. Suivez plutôt les étapes de la dernière version de AWS WAF, à l'adresseConfiguration de votre compte pour utiliser les services.

Une fois ces étapes terminées, reportez-vous Commencer à utiliser AWS WAF Classic à la section pour continuer à démarrer avec AWS WAF Classic.

> **Note**
>
> AWS Shield Standard est inclus dans la AWS WAF version classique et ne nécessite aucune configuration supplémentaire. Pour plus d’informations, consultez Comment fonctionnent AWS Shield et Shield Advanced.

Avant d'utiliser AWS WAF Classic ou AWS Shield Advanced pour la première fois, suivez les étapes décrites dans cette section.

Rubriques

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez https://portal.aws.amazon.com/billing/signup.
2. Suivez les instructions en ligne.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique et vous saisirez un code de vérification en utilisant le clavier numérique du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. Pour des raisons de sécurité, attribuez un accès administratif à un utilisateur et utilisez uniquement l'utilisateur root pour effectuer les tâches nécessitant un accès utilisateur root.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. Vous pouvez afficher l'activité en cours de votre compte et gérer votre compte à tout moment en accédant à https://aws.amazon.com/ et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .

2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Dans IAM Identity Center, accordez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connectez-vous en tant qu'utilisateur disposant d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribuer l'accès à des utilisateurs supplémentaires

1. Dans IAM Identity Center, créez un ensemble d'autorisations conforme aux meilleures pratiques en matière d'application des autorisations du moindre privilège.

   Pour obtenir des instructions, voir Création d'un ensemble d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

2. Affectez des utilisateurs à un groupe, puis attribuez un accès d'authentification unique au groupe.

Pour obtenir des instructions, voir Ajouter des groupes dans le guide de AWS IAM Identity Center l'utilisateur.

Télécharger les outils

AWS Management Console Il inclut une console pour AWS WAF Classic, mais si vous souhaitez accéder à AWS WAF Classic par programmation, consultez ce qui suit :

- Si vous souhaitez appeler l'API AWS WAF classique sans avoir à gérer des détails de bas niveau tels que l'assemblage de requêtes HTTP brutes, vous pouvez utiliser un AWS SDK. Les AWS SDK fournissent des fonctions et des types de données qui encapsulent les fonctionnalités de AWS WAF Classic et d'autres AWS services. Pour télécharger un AWS SDK, consultez la page correspondante, qui inclut également les prérequis et les instructions d'installation :
  - Java
  - JavaScript
  - .NET
  - Node.js
  - PHP
  - Python
  - Ruby

  Pour obtenir la liste complète des AWS SDK, consultez la section Outils pour Amazon Web Services.
- Si vous utilisez un langage de programmation pour lequel aucun SDK AWS n'est fourni, la référence des AWS WAF API documente les opérations prises en charge par AWS WAF Classic.
- Le AWS Command Line Interface (AWS CLI) est compatible avec AWS WAF Classic. Vous AWS CLI permet de contrôler plusieurs AWS services à partir de la ligne de commande et de les automatiser par le biais de scripts. Pour plus d'informations, consultez AWS Command Line Interface.
- AWS Tools for Windows PowerShell prend en charge AWS WAF Classic. Pour plus d'informations, consultez le Guide de référence des cmdlets AWS Tools for PowerShell.

Comment fonctionne AWS WAF Classic

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Vous utilisez AWS WAF Classic pour contrôler la façon dont API Gateway, Amazon CloudFront ou un Application Load Balancer répondent aux requêtes Web. Vous commencez par créer des conditions, des règles et des listes de contrôle d'accès web (ACL). Vous définissez vos conditions, combinez vos conditions en règles et combinez les règles en une liste ACL web.

> **Note**
>
> Vous pouvez également utiliser AWS WAF Classic pour protéger vos applications hébergées dans des conteneurs Amazon Elastic Container Service (Amazon ECS). Amazon ECS est un service de gestion de conteneurs rapide et hautement évolutif qui facilite l'exécution, l'arrêt et la gestion des conteneurs Docker sur un cluster. Pour utiliser cette option, vous configurez Amazon ECS de manière à utiliser un Application Load Balancer compatible avec AWS WAF Classic afin d'acheminer et de protéger le trafic HTTP/HTTPS (couche 7) entre les tâches de votre service. Pour plus d'informations, consultez la rubrique Service Load Balancing dans le manuel Amazon Elastic Container Service Developer Guide.

Conditions

Les conditions définissent les caractéristiques de base que vous souhaitez que AWS WAF Classic surveille dans les requêtes Web :

- Les scripts qui sont susceptibles d'être malveillants. Les pirates intègrent des scripts qui peuvent exploiter les vulnérabilités des applications web. Il s'agit de scripts inter-sites.
- Les adresses IP ou les plages d'adresses IP d'où proviennent les requêtes.
- Pays ou emplacement géographique d'où proviennent les demandes.

- La longueur des parties spécifiées de la requête, telles que la chaîne de requête.
- Le code SQL susceptible d'être malveillants. Les pirates essaient d'extraire les données de votre base de données en intégrant un code SQL malveillant dans une requête web. Cette opération s'appelle injection SQL.
- Les chaînes qui apparaissent dans la requête, par exemple, les valeurs qui apparaissent dans l'en-tête `User-Agent` ou les chaînes de texte qui apparaissent dans la chaîne de requête. Vous pouvez également utiliser des expressions régulières (regex) pour spécifier ces chaînes.

Certaines conditions prennent plusieurs valeurs. Par exemple, vous pouvez spécifier jusqu'à 10 000 adresses IP ou plages d'adresses IP dans une condition IP.

Règles

Vous combinez les conditions dans des règles pour cibler précisément les demandes que vous souhaitez autoriser, bloquer ou compter. AWS WAF Classic propose deux types de règles :

Règle régulière

Les règles régulières utilisent uniquement des conditions pour cibler des requêtes spécifiques. Par exemple, en fonction des requêtes récentes que vous avez vu d'un pirate, vous pouvez créer une règle qui inclut les conditions suivantes :

- Les requêtes proviennent de 192.0.2.44.
- Elles contiennent la valeur `BadBot` dans l'en-tête `User-Agent`.
- Elles semblent inclure du code de type SQL dans la chaîne de requête.

Lorsqu'une règle inclut plusieurs conditions, comme dans cet exemple, AWS WAF Classic recherche les demandes qui répondent à toutes les conditions, c'est-à-dire qu'il s'agit `AND` des conditions réunies.

Ajoutez au moins une condition à une règle régulière. Une règle régulière sans condition ne peut correspondre à aucune demande. L'action de la règle (autorisation, décompte ou blocage) n'est donc jamais déclenchée.

Règle basée sur un débit

Les règles basées sur le débit sont similaires aux règles régulières avec en plus une limite de débit. Une règle basée sur le débit compte les demandes provenant d'adresses IP qui satisfont les conditions de la règle. Si les demandes provenant d'une adresse IP dépassent la limite de débit au cours d'une période de cinq minutes, la règle peut déclencher une action. Cela peut prendre une minute ou deux pour que l'action se déclenche.

Les conditions sont facultatives pour les règles basées sur le débit. Si vous n'ajoutez aucune condition dans une règle basée sur le débit, la limite de débit s'applique à toutes les adresses IP. Si vous combinez des conditions avec la limite de débit, cette dernière s'applique aux adresses IP qui correspondent aux conditions.

Par exemple, en fonction des requêtes récentes que vous avez vu d'un pirate, vous pouvez créer une règle basée sur un débit qui inclut les conditions suivantes :

- Les requêtes proviennent de 192.0.2.44.
- Elles contiennent la valeur `BadBot` dans l'en-tête `User-Agent`.

Dans cette règle basée sur un débit, vous pouvez également définir une limite de débit. Dans cet exemple, supposons que vous créiez la limite de débit 1000. Les requêtes qui répondent aux conditions précédentes et qui dépassent 1000 demandes par période de cinq minutes déclenchent l'action de la règle (bloquer ou compter) qui est définie dans la liste ACL Web.

Les demandes qui ne répondent pas aux deux conditions ne sont pas comptabilisées dans la limite de débit et ne sont pas affectées par cette règle.

Comme deuxième exemple, supposons que vous souhaitiez limiter les requêtes vers une page particulière sur votre site Web. Pour ce faire, vous pouvez ajouter la condition de correspondance de chaîne suivante à une règle basée sur un débit :

- La Part of the request to filter on est `URI`.
- Le Match Type (Type de correspondance) est `Starts with`.
- Une Value to match est `login`.

De plus, vous spécifiez 1000 comme `RateLimit`.

En ajoutant cette règle basée sur un débit à une liste ACL web, vous pouvez limiter les requêtes vers votre page de connexion sans affecter le reste de votre site.

Liste ACL web

Une fois que vous avez combiné vos conditions en règles, vous combinez les règles en une liste ACL web. C'est ici que vous définissez une action pour chaque règle (autoriser, bloquer ou compter), ainsi qu'une action par défaut :

Une action pour chaque règle

Lorsqu'une requête Web répond à toutes les conditions d'une règle, AWS WAF Classic peut soit bloquer la demande, soit autoriser son transfert vers l'API API Gateway, la CloudFront

distribution ou un Application Load Balancer. Vous spécifiez l'action que AWS WAF Classic doit exécuter pour chaque règle.

AWS WAF Classic compare une demande aux règles d'une ACL Web dans l'ordre dans lequel vous les avez listées. AWS WAF Classic exécute ensuite l'action associée à la première règle à laquelle la demande correspond. Par exemple, si une requête Web correspond à une règle autorisant les demandes et à une autre règle bloquant les demandes, AWS WAF Classic autorisera ou bloquera la demande en fonction de la règle répertoriée en premier.

Si vous souhaitez tester une nouvelle règle avant de commencer à l'utiliser, vous pouvez également configurer AWS WAF Classic pour compter les demandes répondant à toutes les conditions de la règle. Comme pour les règles qui autorisent ou bloquent des requêtes, une règle qui compte les requêtes est affectée par sa position dans la liste des règles de la liste ACL web. Par exemple, si une requête web correspond à une règle qui autorise les requêtes et à une autre règle qui compte les requêtes, et si la règle qui autorise les requêtes apparaît en premier, la requête n'est pas comptée.

Action par défaut

L'action par défaut détermine si AWS WAF Classic autorise ou bloque une demande qui ne répond à toutes les conditions d'aucune des règles de l'ACL Web. Par exemple, supposons que vous créez une liste ACL web et que vous ajoutez uniquement la règle que vous avez définie précédemment :

- Les requêtes proviennent de 192.0.2.44.
- Elles contiennent la valeur `BadBot` dans l'en-tête `User-Agent`.
- Elles semblent inclure du code SQL malveillant dans la chaîne de requête.

Si une demande ne répond pas aux trois conditions de la règle et si l'action par défaut est la `ALLOW` suivante, AWS WAF Classic transmet la demande à API Gateway CloudFront ou à un Application Load Balancer, et le service répond avec l'objet demandé.

Si vous ajoutez deux règles ou plus à une ACL Web, AWS WAF Classic exécute l'action par défaut uniquement si une demande ne répond à toutes les conditions d'aucune des règles. Par exemple, supposons que vous ajoutez une deuxième règle qui contient une condition :

- Requêtes qui contiennent la valeur `BIGBadBot` dans l'en-tête `User-Agent`.

AWS WAF Classic exécute l'action par défaut uniquement lorsqu'une demande ne répond pas aux trois conditions de la première règle et ne répond pas à l'une des conditions de la seconde règle.

Dans certains cas, une erreur interne AWS WAF peut retarder la réponse à Amazon API Gateway, à Amazon CloudFront ou à un Application Load Balancer concernant l'autorisation ou le blocage d'une demande. Dans ces cas, CloudFront ils autorisent généralement la demande ou diffusent le contenu. API Gateway et un équilibreur de charge d'application rejettent habituellement la requête et ne diffusent pas le contenu.

AWS WAF Tarification classique

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Avec AWS WAF Classic, vous ne payez que pour les ACL et les règles Web que vous créez, ainsi que pour le nombre de requêtes HTTP inspectées par AWS WAF Classic. Pour plus d'informations, consultez la section Tarification AWS WAF classique.

Commencer à utiliser AWS WAF Classic

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Ce didacticiel explique comment utiliser AWS WAF Classic pour effectuer les tâches suivantes :

- Configurez AWS WAF Classic.
- Créez une liste de contrôle d'accès Web (ACL Web) à l'aide de la console AWS WAF Classic et spécifiez les conditions que vous souhaitez utiliser pour filtrer les requêtes Web. Par exemple, vous pouvez spécifier les adresses IP d'où proviennent les requêtes et les valeurs des requêtes qui sont utilisées uniquement par les pirates.
- Ajouter les conditions à une règle. Les règles vous permettent de cibler les requêtes web que vous souhaitez bloquer ou autoriser. Une demande Web doit répondre à toutes les conditions d'une règle avant que AWS WAF Classic ne bloque ou n'autorise les demandes en fonction des conditions que vous spécifiez.
- Ajouter les règles à votre liste ACL web. C'est là que vous spécifiez si vous souhaitez bloquer les requêtes web ou les autoriser en fonction des conditions que vous ajoutez à chaque règle.
- Spécifier une action par défaut, soit bloquer soit autoriser. Il s'agit de l'action que AWS WAF Classic exécute lorsqu'une requête Web ne correspond à aucune de vos règles.
- Choisissez la CloudFront distribution Amazon pour laquelle vous souhaitez que AWS WAF Classic inspecte les requêtes Web. Ce didacticiel couvre les étapes uniquement pour CloudFront, mais le processus pour un Application Load Balancer et les API Amazon API Gateway est essentiellement le même. AWS WAF CloudFront La forme classique est disponible pour tous Régions AWS. AWS WAF La version Classic, destinée à être utilisée avec API Gateway ou un Application Load Balancer, est disponible dans les régions répertoriées sur les points de terminaison du AWS service.

> **Note**
>
> AWS vous facture généralement moins de 0,25 USD par jour pour les ressources que vous créez au cours de ce didacticiel. Lorsque vous avez terminé les opérations dans le cadre de ce didacticiel, nous vous recommandons de supprimer les ressources pour éviter de générer des frais supplémentaires.

Rubriques

Étape 1 : configurer AWS WAF Classic

Si vous n'avez pas encore suivi les étapes générales de configurationConfiguration de AWS WAF Classic, faites-le maintenant.

Étape 2 : Créer une liste ACL web

La console AWS WAF Classic vous guide tout au long du processus de configuration de AWS WAF Classic pour bloquer ou autoriser les requêtes Web en fonction de conditions que vous spécifiez, telles que les adresses IP d'origine des demandes ou les valeurs figurant dans les demandes. Au cours de cette étape, vous créez une liste ACL Web.

Pour créer une liste ACL web

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.

2. Si c'est la première fois que vous utilisez la AWS WAF version classique, choisissez Passer à la AWS WAF version classique, puis sélectionnez Configurer l'ACL Web.

   Si vous avez déjà utilisé AWS WAF Classic, choisissez Web ACL dans le volet de navigation, puis choisissez Create Web ACL.

3. Sur la page Name web ACL (Nommer la liste ACL Web), saisissez un nom dans le champ Web ACL name (Nom de la liste ACL Web).

> **Note**
>
> Vous ne pouvez pas modifier le nom une fois que vous créez la liste ACL web.

4. Pour le nom de la CloudWatch métrique, entrez un nom. Le nom peut contenir uniquement des caractères alphanumériques (A-Z, a-z, 0-9). Il ne peut pas contenir d'espaces.

> **Note**
>
> Vous ne pouvez pas modifier le nom une fois que vous créez la liste ACL web.

5. Choisissez une région dans Région . Si vous souhaitez associer cette ACL Web à une CloudFront distribution, choisissez Global (CloudFront).
6. Pour AWS resource to associate, choisissez la ressource que vous souhaitez associer à votre liste ACL web, puis choisissez Next.

Étape 3 : Créer une condition de correspondance IP

Une condition de correspondance IP spécifie les adresses IP ou les plages d'adresses IP d'où proviennent les requêtes. Au cours de cette étape, vous créez une condition de correspondance IP. Lors d'une étape ultérieure, vous indiquerez si vous souhaitez autoriser ou bloquer les requêtes provenant des adresses IP spécifiées.

> **Note**
>
> Pour plus d'informations sur les conditions de correspondance IP, consultez Utilisation des conditions de correspondance IP.

Pour créer une condition de correspondance IP

1. Sur la page Create conditions, pour IP match conditions, choisissez Create condition.
2. Dans la boîte de dialogue Create IP match condition (Créer une condition de correspondance IP) saisissez un nom dans Name (Nom). Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./.
3. Dans Address (Adresse), saisissez 192.0.2.0/24. Cette plage d'adresses IP, spécifiée en notation CIDR, inclut les adresses IP de 192.0.2.0 à 192.0.2.255. (La plage d'adresses

IP 192.0.2.0/24 est réservée pour obtenir des exemples, donc aucune requête web ne proviendra de ces adresses IP).

AWS WAF Classic prend en charge les plages d'adresses IPv4 : /8 et toute plage comprise entre /16 et /32. AWS WAF Classic prend en charge les plages d'adresses IPv6 : /24, /32, /48, /56, /64 et /128. (Pour spécifier une seule adresse IP, telle que 192.0.2.44, saisissez 192.0.2.44/32.) Les autres plages ne sont pas prises en charge.

Pour plus d'informations sur la notation CIDR, consultez l'article Classless Inter-Domain Routing sur Wikipédia (en anglais).

4. Choisissez Créer.

Étape 4 : Créer une condition de correspondance géographique

Une condition de correspondance géographique spécifie le ou les pays d'où proviennent les demandes. Au cours de cette étape, vous créez une condition de correspondance géographique. Lors d'une étape ultérieure, vous indiquerez si vous souhaitez autoriser ou bloquer les demandes provenant des pays spécifiés.

> **Note**
>
> Pour plus d'informations sur les conditions de correspondance géographique, consultez Utilisation des conditions de correspondance géographique.

Pour créer une condition de correspondance géographique

1. Sur la page Create conditions, pour Geo match conditions, choisissez Create condition.
2. Dans la boîte de dialogue Create geo match condition (Créer une condition de correspondance géographique), saisissez un nom dans Name (Nom). Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./.
3. Choisissez un Location type et un pays. Actuellement, le Type d'emplacement ne peut être que Pays.
4. Choisissez Add location.
5. Choisissez Créer.

Étape 5 : Créer une condition de correspondance de chaîne

Une condition de correspondance de chaîne identifie les chaînes que vous souhaitez que AWS WAF Classic recherche dans une demande, telles qu'une valeur spécifiée dans un en-tête ou dans une chaîne de requête. Généralement, une chaîne est composée de caractères ASCII imprimables, mais vous pouvez spécifier n'importe quel caractère de valeur hexadécimale 0x00 à 0xFF (de valeur décimale 0 à 255). Au cours de cette étape, vous créez une condition de correspondance de chaîne. Lors d'une étape ultérieure, vous spécifierez si vous voulez autoriser ou bloquer les requêtes contenant les chaînes spécifiées.

> **Note**
>
> Pour plus d'informations sur les conditions de correspondance de chaîne, consultez Utilisation des conditions de correspondance de chaîne.

Pour créer une condition de correspondance de chaîne

1. Sur la page Create conditions (Créer des conditions), pour String and regex match conditions (Conditions de correspondance de chaîne et d'expression régulière), choisissez Create condition (Créer une condition).
2. Dans la boîte de dialogue Create string match condition (Créer une condition de correspondance de chaîne), saisissez les valeurs suivantes :

   Nom

   Entrez un nom. Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./.

   Type

   Choisissez String match.

   Partie de la requête à filtrer

   Choisissez la partie de la requête Web que AWS WAF Classic doit inspecter pour une chaîne spécifiée.

   Pour cet exemple, choisissez Header.

> **Note**
>
> Si vous choisissez Body pour la valeur d'une partie de la demande à filtrer, AWS WAF Classic inspecte uniquement les 8 192 premiers octets (8 Ko) car CloudFront seuls les 8 192 premiers octets sont transférés pour inspection. Pour autoriser ou bloquer les demandes dont le corps est supérieur à 8 192 octets, vous pouvez créer une condition de contrainte de taille. (AWS WAF Classic obtient la longueur du corps à partir des en-têtes de requête.) Pour plus d'informations, consultez Utilisation des conditions de contrainte de taille.

En-tête (obligatoire si « Part of the request to filter on » est défini sur « Header »)

Comme vous avez choisi En-tête pour une partie de la demande à filtrer, vous devez spécifier l'en-tête que AWS WAF Classic doit inspecter. Saisissez User-Agent (Utilisateur-Agent). (Cette valeur n'est pas sensible à la casse).

Type de correspondance

Choisissez où la chaîne spécifiée doit apparaître dans l'en-tête User-Agent, par exemple au début, à la fin, ou n'importe où dans la chaîne.

Pour cet exemple, choisissez Exactly matches, ce qui indique que AWS WAF Classic inspecte les requêtes Web à la recherche d'une valeur d'en-tête identique à la valeur que vous spécifiez.

Transformation

Afin de contourner AWS WAF Classic, les attaquants utilisent un formatage inhabituel dans les requêtes Web, par exemple en ajoutant un espace blanc ou en codant l'URL d'une partie ou de la totalité de la demande. Les transformations convertissent la requête web dans un format plus standard en supprimant les espaces, en décodant l'URL de la requête, ou en exécutant d'autres opérations qui éliminent une grande partie du formatage inhabituel que les pirates utilisent couramment.

Vous ne pouvez spécifier qu'un seul type de transformation de texte.

Pour cet exemple, choisissez None.

La valeur est codée en base64

Lorsque la valeur que vous saisissez dans Value to match (Valeur de correspondance) est déjà codée en base64, cochez cette case.

Pour cet exemple, ne cochez pas la case.

Value to match

Spécifiez la valeur que vous souhaitez que AWS WAF Classic recherche dans la partie des requêtes Web que vous avez indiquée dans Partie de la demande à filtrer.

Pour cet exemple, entrez BadBot. AWS WAF Classic inspectera l'`User-Agent`en-tête des requêtes Web pour en déterminer la valeur BadBot.

La longueur maximale de Value to match est 50 caractères. Si vous souhaitez spécifier une valeur codée en base64, vous pouvez fournir jusqu'à 50 caractères avant l'encodage.

3. Si vous souhaitez que AWS WAF Classic inspecte les requêtes Web à la recherche de plusieurs valeurs, telles qu'un `User-Agent` en-tête contenant `BadBot` et une chaîne de requête contenant`BadParameter`, vous avez deux choix :

   - Si vous voulez autoriser ou bloquer des requêtes web uniquement lorsqu'elles contiennent les deux valeurs (`AND`), vous créez une condition de correspondance de chaîne pour chaque valeur.
   - Si vous voulez autoriser ou bloquer des requêtes web lorsqu'elles contiennent une des deux valeurs ou les deux (`OR`), vous ajoutez les deux valeurs à la même condition de correspondance de chaîne.

   Pour cet exemple, choisissez Create.

Étape 5A : Créer une condition d'expression régulière (facultatif)

Une condition d'expression régulière est un type de condition de correspondance de chaîne similaire en ce sens qu'elle identifie les chaînes que vous souhaitez que AWS WAF Classic recherche dans une demande, telles qu'une valeur spécifiée dans un en-tête ou dans une chaîne de requête. La principale différence réside dans le fait que vous utilisez une expression régulière (regex) pour spécifier le modèle de chaîne que vous souhaitez que AWS WAF Classic recherche. Au cours de cette étape, vous créez une condition de correspondance d'expression régulière. Lors d'une étape

ultérieure, vous spécifierez si vous voulez autoriser ou bloquer les requêtes contenant les chaînes spécifiées.

> **Note**
>
> Pour plus d'informations sur les conditions de correspondance d'expression régulière, consultez Utilisation des conditions de correspondance d'expression régulière.

Pour créer une condition de correspondance d'expression régulière

1. Sur la page Create conditions (Créer des conditions), pour String match and regex conditions (Conditions de correspondance de chaîne et d'expression régulière), choisissez Create condition (Créer une condition).
2. Dans la boîte de dialogue Create string match condition (Créer une condition de correspondance de chaîne), saisissez les valeurs suivantes :

   Nom

   Entrez un nom. Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./.

   Type

   Choisissez Regex match.

   Partie de la requête à filtrer

   Choisissez la partie de la requête Web que AWS WAF Classic doit inspecter pour une chaîne spécifiée.

   Pour cet exemple, choisissez Body.

   > **Note**
   >
   > Si vous choisissez Body pour la valeur d'une partie de la demande à filtrer, AWS WAF Classic inspecte uniquement les 8 192 premiers octets (8 Ko) car CloudFront seuls les 8 192 premiers octets sont transférés pour inspection. Pour autoriser ou bloquer les demandes dont le corps est supérieur à 8 192 octets, vous pouvez créer une condition de contrainte de taille. (AWS WAF Classic obtient la longueur du corps

à partir des en-têtes de requête.) Pour plus d'informations, consultez Utilisation des conditions de contrainte de taille.

Transformation

Afin de contourner AWS WAF Classic, les attaquants utilisent un formatage inhabituel dans les requêtes Web, par exemple en ajoutant un espace blanc ou en codant l'URL d'une partie ou de la totalité de la demande. Les transformations convertissent la requête web dans un format plus standard en supprimant les espaces, en décodant l'URL de la requête, ou en exécutant d'autres opérations qui éliminent une grande partie du formatage inhabituel que les pirates utilisent couramment.

Vous ne pouvez spécifier qu'un seul type de transformation de texte.

Pour cet exemple, choisissez None.

Modèles d'expression régulière pour correspondre aux demandes

Choisissez Create regex pattern set.

Nouveau nom d'ensemble de modèles

Entrez un nom, puis spécifiez le modèle d'expression régulière que vous souhaitez que AWS WAF Classic recherche.

Entrez ensuite l'expression régulière I [a@] mAB [a@] dRequest. AWS WAF Classic inspectera l'`User-Agent`en-tête des requêtes Web pour les valeurs suivantes :

- Iama BadRequest
- IamAB@dRequest
- Je @mA BadRequest
- I@mAB@dRequest

3. Choisissez Create pattern set and add filter.
4. Choisissez Créer.

Étape 6 : Créer une condition de correspondance d'injection SQL

Une condition de correspondance par injection SQL identifie la partie des requêtes Web, telle qu'un en-tête ou une chaîne de requête, que AWS WAF Classic doit inspecter pour détecter la présence

de code SQL malveillant. Les pirates utilisent des requêtes SQL pour extraire des données de votre base de données. Au cours de cette étape, vous créez une condition de correspondance d'injection SQL. Au cours d'une étape ultérieure, vous spécifierez si vous souhaitez autoriser ou bloquer les requêtes qui semblent contenir du code SQL malveillant.

> **Note**
>
> Pour plus d'informations sur les conditions de correspondance de chaîne, consultez Utilisation des conditions de correspondance d'injection SQL.

Pour créer une condition de correspondance d'injection SQL

1. Sur la page Create conditions, pour SQL injection match conditions, choisissez Create condition.
2. Dans la boîte de dialogue Create SQL injection match condition (Créer une condition de correspondance d'injection SQL), saisissez les valeurs suivantes :

   Nom

   Entrez un nom.

   Partie de la requête à filtrer

   Choisissez la partie des requêtes Web que AWS WAF Classic doit inspecter pour détecter la présence de code SQL malveillant.

   Pour cet exemple, choisissez Query string.

   > **Note**
   >
   > Si vous choisissez Body pour la valeur d'une partie de la demande à filtrer, AWS WAF Classic inspecte uniquement les 8 192 premiers octets (8 Ko) car CloudFront seuls les 8 192 premiers octets sont transférés pour inspection. Pour autoriser ou bloquer les demandes dont le corps est supérieur à 8 192 octets, vous pouvez créer une condition de contrainte de taille. (AWS WAF Classic obtient la longueur du corps à partir des en-têtes de requête.) Pour plus d'informations, consultez Utilisation des conditions de contrainte de taille.

Transformation

Pour cet exemple, choisissez URL decode.

Les attaquants utilisent un formatage inhabituel, tel que le codage d'URL, afin de contourner AWS WAF Classic. L'option de décodage d'URL élimine une partie de ce formatage dans la requête Web avant que AWS WAF Classic n'inspecte la demande.

Vous ne pouvez spécifier qu'un seul type de transformation de texte.

3. Choisissez Créer.
4. Choisissez Suivant.

Étape 7 : (Facultatif) Créer des conditions supplémentaires

AWS WAF La version classique inclut d'autres conditions, notamment les suivantes :

- Conditions de contrainte de taille : identifie la partie des requêtes Web, telle qu'un en-tête ou une chaîne de requête, dont la longueur AWS WAF doit être vérifiée par Classic. Pour plus d’informations, consultez Utilisation des conditions de contrainte de taille.
- Conditions de correspondance des scripts intersites : identifie la partie des requêtes Web, telle qu'un en-tête ou une chaîne de requête, que vous souhaitez inspecter AWS WAF pour détecter la présence de scripts malveillants. Pour plus d’informations, consultez Utilisation des conditions de correspondance de scripts inter-site.

Vous pouvez créer ces conditions maintenant si vous le souhaitez, ou vous pouvez passer à Étape 8 : Créer une règle et ajouter des conditions.

Étape 8 : Créer une règle et ajouter des conditions

Vous créez une règle pour spécifier les conditions que vous souhaitez que AWS WAF Classic recherche dans les requêtes Web. Si vous ajoutez plusieurs conditions à une règle, une demande Web doit répondre à toutes les conditions de la règle pour que AWS WAF Classic autorise ou bloque les demandes en fonction de cette règle.

> **Note**
>
> Pour plus d'informations sur les règles, consultez Utilisation des règles.

Pour créer une règle et ajouter des conditions

1. Sur la page Create rules, choisissez Create rule.
2. Dans la boîte de dialogue Create rule (Créer une règle), saisissez les valeurs suivantes :

   Nom

   Entrez un nom.

   CloudWatch nom de la métrique

   Entrez le nom de la CloudWatch métrique que AWS WAF Classic créera et associera à la règle. Le nom peut contenir uniquement des caractères alphanumériques (A-Z, a-z, 0-9). Il ne peut pas contenir d'espaces.

   Type de règle

   Choisissez Regular rule (Règle régulière) ou Rate-based rule (Règle basée sur un débit). Les règles basées sur le débit sont identiques aux règles régulières, mais elles prennent également en compte le nombre de requêtes en provenance de l'adresse IP identifiée au cours d'une période de cinq minutes. Pour de plus amples informations sur les types de règle, veuillez consulter Comment fonctionne AWS WAF Classic. Pour cet exemple, choisissez `Regular rule`.

   Limite de débit

   Pour une règle basée sur le débit, saisissez le nombre maximal de requêtes à autoriser par période de cinq minutes provenant d'une adresse IP correspondant aux conditions de la règle.
3. Pour la première condition que vous voulez ajouter à la règle, spécifiez les paramètres suivants :

   - Choisissez si vous souhaitez que AWS WAF Classic autorise ou bloque les demandes selon qu'une demande Web correspond ou non aux paramètres de la condition.

     Pour cet exemple, choisissez does.

- Choisissez le type de condition que vous voulez ajouter à la règle : une condition de jeu de correspondance IP, une condition de jeu de correspondance de chaînes ou une condition d'ensemble de correspondance d'injection SQL.

  Pour cet exemple, choisissez originate from IP addresses in.

- Choisissez la condition que vous souhaitez ajouter à la règle.

  Pour cet exemple, sélectionnez la condition de correspondance IP que vous avez créée dans les tâches précédentes.

4. Choisissez Ajouter une condition.
5. Ajoutez la condition de correspondance géographique que vous avez créée plus tôt. Indiquez l'une des valeurs suivantes :

   - Quand une requête
   - proviennent d'un emplacement géographique dans
   - Choisissez votre condition de correspondance géographique.

6. Choisissez Add another condition.
7. Ajoutez la condition de correspondance de chaîne que vous avez créée plus tôt. Indiquez l'une des valeurs suivantes :

   - Quand une requête
   - correspond au moins à un des filtres dans la condition de correspondance de chaîne
   - Choisissez votre condition de correspondance de chaîne.

8. Choisissez Ajouter une condition.
9. Ajoutez la condition de correspondance d'injection SQL que vous avez créée plus tôt. Indiquez l'une des valeurs suivantes :

   - Quand une requête
   - correspond au moins à un des filtres dans la condition de correspondance d'injection SQL
   - Choisissez votre condition de correspondance d'injection SQL.

10. Choisissez Ajouter une condition.
11. Ajoutez la condition de contrainte de taille que vous avez créée plus tôt. Indiquez l'une des valeurs suivantes :

    - Quand une requête

- correspond au moins à un des filtres dans la condition de contrainte de taille
- Choisissez votre condition de contrainte de taille.

12. Si vous avez créé d'autres conditions, comme une condition d'expression régulière, ajoutez-les de manière similaire.
13. Choisissez Créer.
14. Pour Default action, choisissez Allow all requests that don't match any rules.
15. Choisissez Review and create.

Étape 9 : Ajouter la règle à une liste ACL web

Lorsque vous ajoutez la règle à une liste ACL web, vous spécifiez les paramètres suivants :

- L'action que vous souhaitez que AWS WAF Classic exécute sur les requêtes Web qui répondent à toutes les conditions de la règle : autoriser, bloquer ou compter les demandes.
- L'action par défaut pour la liste ACL web. Il s'agit de l'action que vous souhaitez que AWS WAF Classic exécute sur les requêtes Web qui ne répondent pas à toutes les conditions de la règle : autoriser ou bloquer les demandes.

AWS WAF Classic commence à bloquer les requêtes CloudFront Web qui répondent à toutes les conditions suivantes (et à toutes les autres que vous pourriez avoir ajoutées) :

- La valeur de l'en-tête `User-Agent` est `BadBot`
- (Si vous avez créé et ajouté la condition d'expression régulière) La valeur de `Body` est l'une des quatre chaînes qui correspond au modèle `I[a@]mAB[a@]dRequest`
- Les requêtes provenant d'adresses IP dans la plage de 192.0.2.0-192.0.2.255
- Les demandes proviennent du pays que vous avez sélectionné dans votre condition de correspondance géographique
- Les requêtes semblent inclure du code SQL malveillant dans la chaîne de requête

AWS WAF Classic permet CloudFront de répondre à toutes les demandes qui ne répondent pas à ces trois conditions.

Étape 10 : Nettoyer vos ressources

Vous avez maintenant terminé le didacticiel. Pour éviter que votre compte n'entraîne des frais supplémentaires liés à la AWS WAF version classique, vous devez nettoyer les objets AWS WAF classiques que vous avez créés. Sinon, vous pouvez modifier la configuration de manière à refléter les requêtes web que vous voulez autoriser, bloquer et compter.

> **Note**
>
> AWS vous facture généralement moins de 0,25 USD par jour pour les ressources que vous créez au cours de ce didacticiel. Lorsque vous avez terminé, nous vous recommandons de supprimer les ressources pour éviter de générer des frais supplémentaires.

Pour supprimer les objets facturés par AWS WAF Classic

1. Dissociez votre ACL Web de votre CloudFront distribution :

   a. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

      Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.

   b. Choisissez le nom de l'ACL Web que vous souhaitez supprimer. Cela ouvre une page contenant les détails de l'ACL Web dans le volet droit.

   c. Dans le volet droit, sous l'onglet Règles, accédez aux AWS ressources utilisant cette section ACL Web. Pour la CloudFront distribution à laquelle vous avez associé l'ACL Web, choisissez le x dans la colonne Type.

2. Supprimer les conditions de votre règle :

   a. Dans le volet de navigation, choisissez Règles.

   b. Sélectionnez la règle que vous avez créée dans le didacticiel.

   c. Choisissez Edit rule.

   d. Choisissez le x à droite de chaque en-tête de condition.

   e. Choisissez Mettre à jour.

3. Supprimer la règle de votre liste ACL web et supprimer la liste ACL web :

a. Dans le volet de navigation, choisissez Web ACLs.

b. Choisissez le nom de l'ACL Web que vous avez créée au cours du didacticiel. Cela ouvre une page contenant les détails de l'ACL Web dans le volet droit.

c. Sous l'onglet Rules, choisissez Edit web ACL.

d. Choisissez le x à droite de l'en-tête de la règle.

e. Choisissez Actions, puis Delete web ACL.

4. Supprimer votre règle :

a. Dans le volet de navigation, choisissez Règles.

b. Sélectionnez la règle que vous avez créée dans le didacticiel.

c. Sélectionnez Delete (Supprimer).

d. Dans la boîte de dialogue Delete, choisissez à nouveau Delete pour confirmer.

AWS WAF Classic ne facture pas les conditions, mais si vous souhaitez terminer le nettoyage, effectuez la procédure suivante pour supprimer les filtres des conditions et supprimer les conditions.

Pour supprimer les filtres et les conditions

1. Supprimer la plage d'adresses IP dans votre condition de correspondance IP et supprimer la condition de correspondance IP :

a. Dans le volet de navigation de la console AWS WAF Classic, sélectionnez les adresses IP.

b. Sélectionnez la condition de correspondance IP que vous avez créée dans le didacticiel.

c. Cochez la case pour la plage d'adresses IP que vous avez ajoutée.

d. Choisissez Delete IP address or range.

e. Dans le volet IP match conditions, choisissez Delete.

f. Dans la boîte de dialogue Delete, choisissez à nouveau Delete pour confirmer.

2. Supprimer le filtre dans votre condition de correspondance d'injection SQL et supprimer la condition de correspondance d'injection SQL :

a. Dans le volet de navigation, choisissez SQL injection.

b. Sélectionnez la condition de correspondance d'injection SQL que vous avez créée dans le didacticiel.

c. Cochez la case pour le filtre que vous avez ajouté.

d. Choisissez Delete filter.

e. Dans le volet SQL injection match conditions, choisissez Delete.

f. Dans la boîte de dialogue Delete, choisissez à nouveau Delete pour confirmer.

3. Supprimer le filtre dans votre condition de correspondance de chaîne et supprimer la condition de correspondance de chaîne :

a. Dans le volet de navigation, sélectionnez String and regex matching.

b. Sélectionnez la condition de correspondance de chaîne que vous avez créée dans le didacticiel.

c. Cochez la case pour le filtre que vous avez ajouté.

d. Choisissez Delete filter.

e. Dans le volet String match conditions, choisissez Delete.

f. Dans la boîte de dialogue Delete, choisissez à nouveau Delete pour confirmer.

4. Si vous en avez créé un, supprimez le filtre de votre condition de correspondance d'expression régulière, ainsi que la condition elle-même :

a. Dans le volet de navigation, sélectionnez String and regex matching.

b. Sélectionnez la condition de correspondance d'expression régulière que vous avez créée dans le didacticiel.

c. Cochez la case pour le filtre que vous avez ajouté.

d. Choisissez Delete filter.

e. Dans le volet Regex match conditions, choisissez Delete.

f. Dans la boîte de dialogue Delete, choisissez à nouveau Delete pour confirmer.

5. Supprimer le filtre de votre condition de contrainte de taille et supprimer la condition de contrainte de taille :

a. Dans le volet de navigation, sélectionnez Size constraints.

b. Sélectionnez la condition de contrainte de taille que vous avez créée dans le tutoriel.

c. Cochez la case pour le filtre que vous avez ajouté.

d. Choisissez Delete filter.

e. Dans le volet Size constraint conditions volet, choisissez Delete.

f. Dans la boîte de dialogue Delete, choisissez à nouveau Delete pour confirmer.

Création et configuration d'une liste de contrôle d'accès web (liste ACL web)

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Une liste de contrôle d'accès Web (ACL Web) vous permet de contrôler avec précision les requêtes Web auxquelles votre API Amazon API Gateway, votre CloudFront distribution Amazon ou Application Load Balancer répondent. Vous pouvez autoriser ou bloquer les types de requêtes suivants :

- proviennent d'une adresse IP ou d'une plage d'adresses IP ;
- Provenir d'un pays ou de pays spécifiques
- Contenir une chaîne spécifiée ou correspondre à un modèle d'expression régulière (regex) d'un ensemble particulier de demandes
- dépassent une longueur spécifiée ;
- contiennent un code SQL malveillant (appelé injection SQL) ;
- contiennent des scripts malveillants (appelés scripts inter-site).

Vous pouvez également tester toute combinaison de ces conditions, ou bloquer ou compter les requêtes web qui non seulement répondent aux conditions définies, mais également qui dépassent un nombre spécifié de requêtes au cours d'une période de 5 minutes.

Pour choisir les requêtes que vous voulez autoriser à accéder à votre contenu ou que vous souhaitez bloquer, effectuez les tâches suivantes :

1. Sélectionnez l'action par défaut, autoriser ou bloquer, pour les requêtes web qui ne correspondent pas à une des conditions que vous spécifiez. Pour plus d'informations, consultez Choix de l'action par défaut pour une liste ACL web.

2. Spécifier les conditions selon lesquelles vous souhaitez autoriser ou bloquer des requêtes :
   - Pour autoriser ou bloquer des requêtes selon qu'elles semblent contenir des scripts malveillants ou non, créez des conditions de correspondance de scripts inter-site. Pour plus d'informations, consultez Utilisation des conditions de correspondance de scripts inter-site.
   - Pour autoriser ou bloquer des requêtes en fonction des adresses IP d'où elles proviennent, créez des conditions de correspondance IP. Pour plus d'informations, consultez Utilisation des conditions de correspondance IP.
   - Pour autoriser ou bloquer les demandes basées sur le pays d'où elles proviennent, créez les conditions de correspondance géographique. Pour plus d'informations, consultez Utilisation des conditions de correspondance géographique.
   - Pour autoriser ou bloquer des requêtes selon qu'elles dépassent une longueur spécifiée ou non, créez des conditions de contrainte de taille. Pour plus d'informations, consultez Utilisation des conditions de contrainte de taille.
   - Pour autoriser ou bloquer des requêtes selon qu'elles semblent contenir du code SQL malveillant ou non, créez des conditions de correspondance d'injection SQL. Pour plus d'informations, consultez Utilisation des conditions de correspondance d'injection SQL.
   - Pour autoriser ou bloquer des requêtes en fonction des chaînes qui apparaissent dans les requêtes, créez les conditions de correspondance de chaîne. Pour plus d'informations, consultez Utilisation des conditions de correspondance de chaîne.
   - Pour autoriser ou bloquer les demandes basées sur un modèle d'expression régulière qui apparaissent dans les demandes, créez les conditions de correspondance d'expression régulière. Pour plus d'informations, consultez Utilisation des conditions de correspondance d'expression régulière.
3. Ajoutez les conditions à une ou plusieurs règles. Si vous ajoutez plusieurs conditions à la même règle, les requêtes Web doivent répondre à toutes les conditions pour que AWS WAF Classic autorise ou bloque les demandes en fonction de la règle. Pour plus d'informations, consultez Utilisation des règles. Le cas échéant, vous pouvez utiliser une règle basée sur le débit au lieu d'une règle régulière pour limiter le nombre de requêtes provenant des adresses IP qui répondent aux conditions.
4. Ajoutez les règles à une liste ACL web. Pour chaque règle, indiquez si vous souhaitez que AWS WAF Classic autorise ou bloque les demandes en fonction des conditions que vous avez ajoutées à la règle. Si vous ajoutez plusieurs règles à une ACL Web, AWS WAF Classic évalue les règles dans l'ordre dans lequel elles sont répertoriées dans l'ACL Web. Pour plus d'informations, consultez Utilisation des listes ACL web.

Lorsque vous ajoutez une nouvelle règle ou que vous mettez à jour des règles existantes, cela peut prendre une minute avant que ces modifications soient actives et apparaissent dans vos listes ACL web et ressources.

Rubriques

Utilisation des conditions

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Spécifier les conditions selon lesquelles vous souhaitez autoriser ou bloquer des requêtes.

- Pour autoriser ou bloquer des requêtes selon qu'elles semblent contenir des scripts malveillants ou non, créez des conditions de correspondance de scripts inter-site. Pour plus d’informations, consultez Utilisation des conditions de correspondance de scripts inter-site.
- Pour autoriser ou bloquer des requêtes en fonction des adresses IP d'où elles proviennent, créez des conditions de correspondance IP. Pour plus d’informations, consultez Utilisation des conditions de correspondance IP.
- Pour autoriser ou bloquer les demandes basées sur le pays d'où elles proviennent, créez les conditions de correspondance géographique. Pour plus d’informations, consultez Utilisation des conditions de correspondance géographique.
- Pour autoriser ou bloquer des requêtes selon qu'elles dépassent une longueur spécifiée ou non, créez des conditions de contrainte de taille. Pour plus d’informations, consultez Utilisation des conditions de contrainte de taille.

- Pour autoriser ou bloquer des requêtes selon qu'elles semblent contenir du code SQL malveillant ou non, créez des conditions de correspondance d'injection SQL. Pour plus d'informations, consultez Utilisation des conditions de correspondance d'injection SQL.
- Pour autoriser ou bloquer des requêtes en fonction des chaînes qui apparaissent dans les requêtes, créez les conditions de correspondance de chaîne. Pour plus d'informations, consultez Utilisation des conditions de correspondance de chaîne.
- Pour autoriser ou bloquer les demandes basées sur un modèle d'expression régulière qui apparaissent dans les demandes, créez les conditions de correspondance d'expression régulière. Pour plus d'informations, voir Utilisation des conditions de correspondance d'expression régulière.

Rubriques

Utilisation des conditions de correspondance de scripts inter-site

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Les pirates insèrent parfois des scripts dans les requêtes web dans le but d'exploiter les vulnérabilités d'applications web. Vous pouvez créer une ou plusieurs conditions de correspondance entre les scripts intersites afin d'identifier les parties des requêtes Web, telles que l'URI ou la chaîne

de requête, que AWS WAF Classic doit inspecter pour détecter d'éventuels scripts malveillants. Ultérieurement dans le processus, lorsque vous créez une liste ACL web, vous spécifiez s'il convient d'autoriser ou de bloquer des requêtes qui semblent contenir des scripts malveillants.

Rubriques

Création de conditions de correspondance de scripts inter-site

Lorsque vous créez des conditions de correspondance de scripts inter-site, vous spécifiez des filtres. Les filtres indiquent la partie des requêtes Web que AWS WAF Classic doit inspecter pour détecter la présence de scripts malveillants, tels que l'URI ou la chaîne de requête. Vous pouvez ajouter plus d'un filtre à une condition de correspondance de scripts inter-sites, ou vous pouvez créer une condition distincte pour chaque filtre. Voici comment chaque configuration affecte le comportement AWS WAF classique :

- Plus d'un filtre par condition de correspondance de script intersite (recommandé) — Lorsque vous ajoutez une condition de correspondance de script intersite contenant plusieurs filtres à une règle et que vous ajoutez la règle à une ACL Web, une demande Web ne doit correspondre qu'à l'un des filtres de la condition de correspondance de script intersite pour que AWS WAF Classic autorise ou bloque la demande en fonction de cette condition.

  Par exemple, supposons que vous créez une condition de correspondance de scripts inter-site et que la condition contient deux filtres. Un filtre demande à AWS WAF Classic d'inspecter l'URI pour détecter la présence de scripts malveillants, et l'autre indique à AWS WAF Classic d'inspecter la chaîne de requête. AWS WAF Classic autorise ou bloque les demandes si elles semblent contenir des scripts malveillants dans l'URI ou dans la chaîne de requête.
- Un filtre par condition de correspondance de script intersite — Lorsque vous ajoutez les conditions de correspondance de scripts intersites distinctes à une règle et que vous ajoutez la règle à une ACL Web, les requêtes Web doivent répondre à toutes les conditions pour que AWS WAF Classic autorise ou bloque les demandes en fonction de ces conditions.

Supposons que vous créez deux conditions et que chaque condition contient l'un des deux filtres de l'exemple précédent. Lorsque vous ajoutez les deux conditions à la même règle et que vous ajoutez la règle à une ACL Web, AWS WAF Classic autorise ou bloque les demandes uniquement lorsque l'URI et la chaîne de requête semblent contenir des scripts malveillants.

> **Note**
>
> Lorsque vous ajoutez une condition de correspondance entre les scripts intersites à une règle, vous pouvez également configurer AWS WAF Classic pour autoriser ou bloquer les requêtes Web qui ne semblent pas contenir de scripts malveillants.

Pour créer une condition de correspondance de scripts inter-site

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez Cross-site scripting.
3. Choisissez Create condition.
4. Indiquez les paramètres de filtre applicables. Pour plus d'informations, consultez Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de correspondance de scripts inter-site.
5. Choisissez Add another filter.
6. Si vous souhaitez ajouter un autre filtre, répétez les étapes 4 et 5.
7. Lorsque vous avez fini d'ajouter les filtres, choisissez Create.

Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de correspondance de scripts inter-site

Lorsque vous créez ou mettez à jour une condition de correspondance de scripts inter-site, vous spécifiez les valeurs suivantes :

Nom

Le nom de la condition de correspondance de scripts inter-site.

Le nom ne peut contenir que les caractères A-Z, a-z, 0-9 et les caractères spéciaux suivants : _-!"#`+*},./ . Vous ne pouvez pas modifier la nom d'une condition après l'avoir créée.

Partie de la requête à filtrer

Choisissez la partie de chaque requête Web que AWS WAF Classic doit inspecter pour détecter la présence de scripts malveillants :

En-tête

Un en-tête de requête spécifié, par exemple, l'en-tête `User-Agent` ou `Referer`. Si vous choisissez Header, précisez le nom de l'en-tête dans le champs Header.

Méthode HTTP

La méthode HTTP, qui indique le type d'opération que la demande demande à l'origine d'effectuer. CloudFront prend en charge les méthodes suivantes : `DELETEGET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, et`PUT`.

Chaîne de requête

La partie d'une URL qui s'affiche après un caractère `?`, le cas échéant.

> **Note**
>
> Pour les conditions de correspondance de scripts inter-site, nous vous recommandons de choisir All query parameters (values only) [Tous les paramètres de requête (valeurs uniquement)] au lieu de Query string (Chaîne de requête) pour Part of the request to filter on (Partie de la requête sur laquelle filtrer).

URI

Le chemin URI de la demande, qui identifie la ressource, par exemple,`/images/daily-ad.jpg`. Cela n'inclut pas la chaîne de requête ou les composants du fragment de l'URI. Pour plus d'informations, voir Uniform Resource Identifier (URI) : syntaxe générique.

À moins qu'une transformation ne soit spécifiée, un URI n'est pas normalisé et est inspecté au moment AWS où il est reçu du client dans le cadre de la demande. Une Transformation reformate l'URI comme spécifié.

Corps de texte

La partie d'une requête qui contient les données supplémentaires que vous souhaitez envoyer à votre serveur web en tant que corps de la requête HTTP, telles que les données d'un formulaire.

> **Note**
>
> Si vous choisissez Body pour la valeur d'une partie de la demande à filtrer, AWS WAF Classic inspecte uniquement les 8 192 premiers octets (8 Ko). Pour autoriser ou bloquer les demandes dont le corps est supérieur à 8 192 octets, vous pouvez créer une condition de contrainte de taille. (AWS WAF Classic obtient la longueur du corps à partir des en-têtes de requête.) Pour plus d'informations, consultez Utilisation des conditions de contrainte de taille.

Paramètre de requête unique (valeur uniquement)

Tous les paramètres que vous avez définis dans le cadre de la chaîne de requête. Par exemple, si l'URL est « www.xyz.com ? UserName =abc& SalesRegion =seattle », vous pouvez ajouter un filtre au paramètre or. UserNameSalesRegion

Si vous choisissez Single query parameter (value only) (Paramètre de requête unique (valeur uniquement)), vous spécifierez également un Query parameter name (Nom du paramètre de requête). Il s'agit du paramètre de la chaîne de requête que vous allez inspecter, tel que UserNameou SalesRegion. La longueur maximale de Query parameter name (Nom du paramètre de requête) est de 30 caractères. Query parameter name (Nom du paramètre de requête) n'est pas sensible à la casse. Par exemple, si vous spécifiez le UserNamenom du paramètre Query, celui-ci correspondra à toutes les variantes de UserName, telles que username et UserName.

Tous les paramètres de requête (valeurs uniquement)

Semblable au paramètre de requête unique (valeur uniquement), mais plutôt que d'inspecter les valeurs d'un seul paramètre, AWS WAF Classic inspecte toutes les valeurs des paramètres de la chaîne de requête pour détecter d'éventuels scripts malveillants. Par exemple, si l'URL est « www.xyz.com ? UserName =abc& SalesRegion =seattle » et que vous choisissez Tous les paramètres de requête (valeurs uniquement), AWS WAF Classic déclenchera une correspondance si la valeur est ou contient d'éventuels scripts malveillants. UserNameSalesRegion

En-tête

Si vous avez choisi En-tête pour une partie de la demande à filtrer, choisissez un en-tête dans la liste des en-têtes courants ou entrez le nom d'un en-tête que AWS WAF Classic doit inspecter pour détecter la présence de scripts malveillants.

Transformation

Une transformation reformate une requête Web avant que AWS WAF Classic ne l'inspecte. Cela élimine une partie du formatage inhabituel utilisé par les attaquants dans les requêtes Web dans le but de contourner AWS WAF Classic.

Vous ne pouvez spécifier qu'un seul type de transformation de texte.

Les transformations peuvent effectuer les opérations suivantes :

Aucun

AWS WAF Classic n'effectue aucune transformation de texte sur la requête Web avant de l'inspecter pour détecter la correspondance de la chaîne dans Value.

Convertir en minuscules

AWS WAF Classic convertit les lettres majuscules (A-Z) en minuscules (a-z).

Décodage d'HTML

AWS WAF Classic remplace les caractères codés en HTML par des caractères non codés :

- Remplace `"` par &
- Remplace ` ` par un espace insécable
- Remplace `<` par <
- Remplace `>` par >
- Remplace les caractères qui sont représentées au format hexadécimal, `&#xhhhh;`, par les caractères correspondants
- Remplace les caractères qui sont représentés au format décimal, `&#nnnn;`, par les caractères correspondants

Normalisation des espaces blancs

AWS WAF Classic remplace les caractères suivants par un espace (32 décimal) :

- \f, saut de page, décimale 12
- \t, tabulation, décimale 9

- \n, nouvelle ligne, décimale 10
- \r, retour chariot, décimale 13
- \v, tabulation verticale, décimale 11
- Espace insécable, décimale 160

En outre, cette option remplace plusieurs espaces par un seul.

Simplifier la ligne de commande

Pour les requêtes qui contiennent des commandes de ligne de commande du système d'exploitation, utilisez cette option pour effectuer les transformations suivantes :

- Supprimer les caractères suivants : \ " ' ^
- Supprimer les espaces avant les caractères suivants : / (
- Remplacer les caractères suivants par un espace : , ;
- Remplacer plusieurs espaces par un espace
- Convertit les lettres majuscules (A-Z) en lettres minuscules (a-z)

Décodage d'URL

Décoder une requête encodée par URL.

Ajout et suppression de filtres dans une condition de correspondance de scripts inter-site

Vous pouvez ajouter ou supprimer des filtres dans une condition de correspondance de scripts inter-site. Pour modifier un filtre, ajoutez un nouveau filtre et supprimez l'ancien.

Pour ajouter ou supprimer des filtres dans une condition de correspondance de scripts inter-site

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez Cross-site scripting.
3. Sélectionnez la condition pour laquelle vous souhaitez ajouter ou supprimer des filtres.
4. Pour ajouter des filtres, effectuez les opérations suivantes :

   a. Choisissez Add filter.

   b. Indiquez les paramètres de filtre applicables. Pour plus d'informations, consultez Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de correspondance de scripts inter-site.
   c. Choisissez Ajouter.
5. Pour supprimer des filtres, effectuez les opérations suivantes :
   a. Sélectionnez le filtre à supprimer.
   b. Choisissez Delete filter.

Suppression de conditions de correspondance de scripts inter-site

Si vous souhaitez supprimer une condition de correspondance de scripts inter-site, vous devez d'abord supprimer tous les filtres de la condition, puis supprimer la condition de toutes les règles qui l'utilisent, comme décrit dans la procédure suivante.

Pour supprimer une condition de correspondance de scripts inter-site

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez Cross-site scripting.
3. Dans le volet Cross-site scripting match conditions, choisissez la condition de correspondance de scripts inter-site que vous souhaitez supprimer.
4. Dans le volet droit, choisissez l'onglet Associated rules.

   Si la liste des règles qui utilisent cette condition de correspondance de scripts inter-site est vide, passez à l'étape 6. Si la liste contient une ou des règles, notez-les et passez à l'étape 5.
5. Pour supprimer la condition de correspondance de scripts inter-site des règles qui l'utilisent, effectuez les opérations suivantes :
   a. Dans le volet de navigation, choisissez Règles.
   b. Choisissez le nom d'une règle qui utilise la condition de correspondance de scripts inter-site que vous souhaitez supprimer.
   c. Dans le volet droit, sélectionnez la condition de correspondance de scripts inter-site que vous souhaitez supprimer de la règle, puis sélectionnez Remove selected condition.

d. Répétez les étapes b et c pour toutes les autres règles qui utilisent la condition de correspondance de scripts inter-site que vous souhaitez supprimer.

e. Dans le volet de navigation, sélectionnez Cross-site scripting.

f. Dans le volet Cross-site scripting match conditions, choisissez la condition de correspondance de scripts inter-site que vous souhaitez supprimer.

6. Choisissez Delete pour supprimer la condition sélectionnée.

Utilisation des conditions de correspondance IP

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Si vous souhaitez autoriser ou bloquer des requêtes web en fonction des adresses IP d'où proviennent les requêtes, créez une ou plusieurs conditions de correspondance IP. Une condition de correspondance IP répertorie jusqu'à 10 000 adresses IP ou plages d'adresses IP d'où proviennent vos requêtes. Ultérieurement dans le processus, lorsque vous créez une liste ACL web, vous spécifiez s'il convient d'autoriser ou de bloquer les requêtes provenant de ces adresses IP.

Rubriques

- Création d'une condition de correspondance IP
- Modification des conditions de correspondance IP
- Suppression des conditions de correspondance IP

Création d'une condition de correspondance IP

Si vous voulez autoriser des requêtes web et en bloquer d'autres en fonction des adresses IP d'où proviennent les requêtes, créez une condition de correspondance IP pour les adresses IP que vous voulez autoriser et une autre condition de correspondance IP pour les adresses IP que vous souhaitez bloquer.

> **Note**
>
> Lorsque vous ajoutez une condition de correspondance IP à une règle, vous pouvez également configurer AWS WAF Classic pour autoriser ou bloquer les requêtes Web qui ne proviennent pas des adresses IP que vous spécifiez dans la condition.

Pour créer une condition de correspondance IP

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez IP addresses.
3. Choisissez Create condition.
4. Saisissez un nom dans le champ Name (Nom).

   Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./. Vous ne pouvez pas modifier la nom d'une condition après l'avoir créée.
5. Sélectionnez la version IP appropriée et spécifiez une adresse IP ou une plage d'adresses IP en utilisant la notation CIDR. Voici quelques exemples :

   - Pour spécifier l'adresse IPv4 192.0.2.44, tapez 192.0.2.44/32.
   - Pour spécifier l'adresse IPv6 0:0:0:0:0:ffff:c000:22c, tapez 0:0:0:0:0:ffff:c000:22c/128.
   - Pour spécifier la plage d'adresses IPv4 de 192.0.2.0 à 192.0.2.255, tapez 192.0.2.0/24.
   - Pour spécifier la plage d'adresses IPv6 de 2620:0:2d0:200:0:0:0:0 à 2620:0:2d0:200:ffff:ffff:ffff:ffff, saisissez 2620:0:2d0:200::/64.

   AWS WAF Classic prend en charge les plages d'adresses IPv4 : /8 et toute plage comprise entre /16 et /32. AWS WAF Classic prend en charge les plages d'adresses IPv6 : /24, /32, /48, /56, /64 et /128. Pour plus d'informations sur la notation CIDR, consultez l'article Classless Inter-Domain Routing sur Wikipédia (en anglais).
6. Choisissez Add another IP address or range.
7. Si vous souhaitez ajouter une autre adresse IP ou une plage, répétez les étapes 5 et 6.

8. Lorsque vous avez fini d'ajouter des valeurs, choisissez Create IP match condition.

Modification des conditions de correspondance IP

Vous pouvez ajouter une plage d'adresses IP à une condition de correspondance IP ou supprimer une plage d'adresses. Pour modifier une plage d'adresses, ajoutez-en une nouvelle et supprimez l'ancienne.

Pour modifier une condition de correspondance IP

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez IP addresses.
3. Dans le volet IP match conditions, sélectionnez la condition de correspondance IP que vous voulez modifier.
4. Pour ajouter une plage d'adresses IP :

   a. Dans le volet droit, sélectionnez Add IP address or range.

   b. Sélectionnez la version IP correcte et saisissez une plage d'adresses IP en utilisant la notation CIDR. Voici quelques exemples :

      - Pour spécifier l'adresse IPv4 192.0.2.44, saisissez 192.0.2.44/32.
      - Pour spécifier l'adresse IPv6 0:0:0:0:0:ffff:c000:22c, saisissez 0:0:0:0:0:ffff:c000:22c/128.
      - Pour spécifier la plage d'adresses IPv4 de 192.0.2.0 à 192.0.2.255, saisissez 192.0.2.0/24.
      - Pour spécifier la plage d'adresses IPv6 de 2620:0:2d0:200:0:0:0:0 à 2620:0:2d0:200:ffff:ffff:ffff:ffff, saisissez 2620:0:2d0:200::/64.

      AWS WAF Classic prend en charge les plages d'adresses IPv4 : /8 et toute plage comprise entre /16 et /32. AWS WAF Classic prend en charge les plages d'adresses IPv6 : /24, /32, /48, /56, /64 et /128. Pour plus d'informations sur la notation CIDR, consultez l'article Classless Inter-Domain Routing sur Wikipédia (en anglais).

c. Pour ajouter d'autres adresses IP, choisissez Add another IP address (Ajouter une autre adresse IP) et saisissez la valeur.

d. Choisissez Ajouter.

5. Pour supprimer une adresse IP ou une plage :

a. Dans le volet droit, sélectionnez les valeurs que vous souhaitez supprimer.

b. Choisissez Delete IP address or range.

Suppression des conditions de correspondance IP

Si vous souhaitez supprimer une condition de correspondance IP, vous devez d'abord supprimer toutes les adresses et plages d'adresses IP de la condition, puis supprimer la condition de toutes les règles qui l'utilisent, comme décrit dans la procédure suivante.

Pour supprimer une condition de correspondance IP

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.

2. Dans le volet de navigation, choisissez IP addresses.

3. Dans le volet IP match conditions, sélectionnez la condition de correspondance IP que vous voulez supprimer.

4. Dans le volet droit, choisissez l'onglet Rules.

   Si la liste des règles utilisant cette condition de correspondance IP est vide, passez à l'étape 6. Si la liste contient une ou des règles, notez-les et passez à l'étape 5.

5. Pour supprimer la condition de correspondance IP des règles qui l'utilisent, effectuez les opérations suivantes :

a. Dans le volet de navigation, choisissez Règles.

b. Choisissez le nom d'une règle qui utilise la condition de correspondance IP que vous souhaitez supprimer.

c. Dans le volet droit, sélectionnez la condition de correspondance IP que vous souhaitez supprimer de la règle, puis sélectionnez Remove selected condition.

d. Répétez les étapes b et c pour toutes les autres règles qui utilisent la condition de correspondance IP que vous souhaitez supprimer.

e. Dans le volet de navigation, sélectionnez IP match conditions.

f. Dans le volet IP match conditions, sélectionnez la condition de correspondance IP que vous voulez supprimer.

6. Choisissez Delete pour supprimer la condition sélectionnée.

Utilisation des conditions de correspondance géographique

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Si vous souhaitez autoriser ou bloquer les demandes web en fonction du pays d'où proviennent les demandes, créez une ou plusieurs conditions de correspondance géographique. Une condition de correspondance géographique répertorie les pays d'où proviennent vos demandes. Ultérieurement dans le processus, lorsque vous créez une liste ACL web, vous spécifiez s'il convient d'autoriser ou de bloquer les demandes provenant de ces pays.

Vous pouvez utiliser les conditions de correspondance géographique avec d'autres conditions ou règles AWS WAF classiques pour créer un filtrage sophistiqué. Par exemple, si vous souhaitez bloquer certains pays, mais continuer à autoriser des adresses IP spécifiques de ce pays, vous pouvez créer une règle contenant une condition de correspondance géographique et une condition de correspondance d'adresse IP. Configurez la règle pour bloquer les demandes en provenance de ce pays et ne correspondant pas aux adresses IP approuvées. Autre exemple, si vous voulez hiérarchiser les ressources pour les utilisateurs d'un pays donné, vous pouvez inclure une condition de correspondance géographique dans deux règles différentes basées sur la fréquence. Définissez une limite de fréquence plus élevée pour les utilisateurs du pays préféré et définissez une limite de fréquence inférieure pour tous les autres utilisateurs.

> **Note**
>
> Si vous utilisez la fonctionnalité CloudFront de restriction géographique pour empêcher un pays d'accéder à votre contenu, toute demande provenant de ce pays est bloquée et n'est pas transmise à AWS WAF Classic. Par conséquent, si vous souhaitez autoriser ou bloquer des demandes en fonction de la géographie ou d'autres conditions AWS WAF classiques, vous ne devez pas utiliser la fonctionnalité CloudFront de restriction géographique. Vous devez plutôt utiliser une condition de correspondance géographique AWS WAF classique.

Rubriques

Création d'une condition de correspondance géographique

Si vous voulez autoriser certaines demandes web et en bloquer d'autres en fonction des pays d'où proviennent les demandes, créez une condition de correspondance géographique pour les pays que vous voulez autoriser et une autre condition de correspondance géographique pour les pays que vous voulez bloquer.

> **Note**
>
> Lorsque vous ajoutez une condition de correspondance géographique à une règle, vous pouvez également configurer AWS WAF Classic pour autoriser ou bloquer les requêtes Web qui ne proviennent pas du pays que vous spécifiez dans la condition.

Pour créer une condition de correspondance géographique

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez Geo match.

3. Choisissez Create condition.
4. Saisissez un nom dans le champ Name (Nom).

   Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./. Vous ne pouvez pas modifier la nom d'une condition après l'avoir créée.
5. Choisissez une Region.
6. Choisissez un Location type et un pays. Letype d'emplacement ne peut actuellement être que Country (Pays).
7. Choisissez Add location.
8. Choisissez Créer.

Modification des conditions de correspondance géographique

Vous pouvez ajouter des pays à votre condition de correspondance géographique ou en supprimer.

Pour modifier une condition de correspondance géographique

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez Geo match.
3. Dans le volet Geo match conditions, sélectionnez la condition de correspondance géographique que vous voulez modifier.
4. Pour ajouter un pays :

   a. Dans le volet droit, choisissez Add filter.

   b. Choisissez un Location type et un pays. Letype d'emplacement ne peut actuellement être que Country (Pays).

   c. Choisissez Ajouter.
5. Pour supprimer un pays :

   a. Dans le volet droit, sélectionnez les valeurs que vous souhaitez supprimer.

   b. Choisissez Delete filter.

Suppression des conditions de correspondance géographique

Si vous souhaitez supprimer une condition de correspondance géographique, vous devez d'abord supprimer tous les pays de la condition, puis supprimer la condition de toutes les règles qui l'utilisent, comme décrit dans la procédure suivante.

Pour supprimer une condition de correspondance géographique

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Supprimez la condition de correspondance géographique des règles qui l'utilisent :
   a. Dans le volet de navigation, choisissez Règles.
   b. Choisissez le nom d'une règle qui utilise la condition de correspondance géographique que vous souhaitez supprimer.
   c. Dans le volet droit, choisissez Edit rule.
   d. Choisissez le X en regard de la condition que vous voulez supprimer.
   e. Choisissez Mettre à jour.
   f. Répétez les étapes pour toutes les autres règles qui utilisent la condition de correspondance géographique que vous souhaitez supprimer.
3. Supprimez les filtres de la condition que vous voulez supprimer :
   a. Dans le volet de navigation, sélectionnez Geo match.
   b. Choisissez le nom de la condition de correspondance géographique que vous souhaitez supprimer.
   c. Dans le volet droit, cochez la case en regard de Filter pour sélectionner tous les filtres.
   d. Choisissez Delete Filter.
4. Dans le volet de navigation, sélectionnez Geo match.
5. Dans le volet Geo match conditions, sélectionnez la condition de correspondance géographique que vous voulez supprimer.
6. Choisissez Delete pour supprimer la condition sélectionnée.

Utilisation des conditions de contrainte de taille

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Si vous souhaitez autoriser ou bloquer des requêtes web en fonction de la longueur de parties spécifiées de requêtes, créez une ou plusieurs conditions de contrainte de taille. Une condition de contrainte de taille identifie la partie des requêtes Web que AWS WAF Classic doit examiner, le nombre d'octets que AWS WAF Classic doit rechercher et un opérateur, tel que supérieur à (>) ou inférieur à (<). Par exemple, vous pouvez utiliser une condition de contrainte de taille pour rechercher des chaînes de requête supérieures à 100 octets. Ultérieurement dans le processus, lorsque vous créez une liste ACL web, vous spécifiez s'il convient d'autoriser ou de bloquer les requêtes en fonction de ces paramètres.

Notez que si vous configurez AWS WAF Classic pour inspecter le corps de la demande, par exemple en recherchant dans le corps une chaîne spécifiée, AWS WAF Classic inspecte uniquement les 8 192 premiers octets (8 Ko). Si le corps de la requête pour vos requêtes web ne dépasse jamais 8 192 octets, vous pouvez créer une condition de contrainte de taille et bloquer les requêtes dont le corps est supérieur à 8 192 octets.

Rubriques

Création de conditions de contrainte de taille

Lorsque vous créez des conditions de contrainte de taille, vous spécifiez des filtres qui identifient la partie des requêtes Web dont vous souhaitez que AWS WAF Classic évalue la longueur. Vous

pouvez ajouter plus d'un filtre à une condition de contrainte de taille ou vous pouvez créer une condition distincte pour chaque filtre. Voici comment chaque configuration affecte le comportement AWS WAF classique :

- Un filtre par condition de contrainte de taille : lorsque vous ajoutez des conditions de contrainte de taille distinctes à une règle et que vous ajoutez la règle à une ACL Web, les requêtes Web doivent répondre à toutes les conditions pour que AWS WAF Classic autorise ou bloque les demandes en fonction de ces conditions.

  Par exemple, supposons que vous créez deux conditions. Une correspond aux requêtes web dont les chaînes de requête sont supérieures à 100 octets. L'autre correspond aux requêtes web dont la taille du corps est supérieure à 1 024 octets. Lorsque vous ajoutez les deux conditions à la même règle et que vous ajoutez la règle à une ACL Web, AWS WAF Classic autorise ou bloque les demandes uniquement lorsque les deux conditions sont vraies.
- Plusieurs filtres par condition de contrainte de taille : lorsque vous ajoutez une condition de contrainte de taille contenant plusieurs filtres à une règle et que vous ajoutez la règle à une ACL Web, il suffit qu'une demande Web corresponde à l'un des filtres de la condition de contrainte de taille pour que AWS WAF Classic autorise ou bloque la demande en fonction de cette condition.

  Supposons que vous créiez une condition au lieu de deux et que celle-ci contienne les deux mêmes filtres que dans l'exemple précédent. AWS WAF Classic autorise ou bloque les demandes si la chaîne de requête est supérieure à 100 octets ou si le corps de la demande est supérieur à 1024 octets.

> **Note**
>
> Lorsque vous ajoutez une condition de contrainte de taille à une règle, vous pouvez également configurer AWS WAF Classic pour autoriser ou bloquer les requêtes Web qui ne correspondent pas aux valeurs de la condition.

Pour créer une condition de contrainte de taille

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.

2. Dans le volet de navigation, sélectionnez Size constraints.
3. Choisissez Create condition.
4. Indiquez les paramètres de filtre applicables. Pour plus d'informations, consultez Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de contrainte de taille.
5. Choisissez Add another filter.
6. Si vous souhaitez ajouter un autre filtre, répétez les étapes 4 et 5.
7. Lorsque vous avez fini d'ajouter des filtres, sélectionnez Create size constraint condition.

Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de contrainte de taille

Lorsque vous créez ou mettez à jour une condition de contrainte de taille, vous spécifiez les valeurs suivantes :

Nom

Saisissez un nom pour la condition de contrainte de taille.

Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./. Vous ne pouvez pas modifier la nom d'une condition après l'avoir créée.

Partie de la requête à filtrer

Choisissez la partie de chaque requête Web dont vous souhaitez que AWS WAF Classic évalue la longueur :

En-tête

Un en-tête de requête spécifié, par exemple, l'en-tête `User-Agent` ou `Referer`. Si vous choisissez Header, précisez le nom de l'en-tête dans le champs Header.

Méthode HTTP

La méthode HTTP, qui indique le type d'opération que la demande demande à l'origine d'effectuer. CloudFront prend en charge les méthodes suivantes : `DELETEGET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, et`PUT`.

Chaîne de requête

La partie d'une URL qui s'affiche après un caractère ?, le cas échéant.

URI

Le chemin URI de la demande, qui identifie la ressource, par exemple,`/images/daily-ad.jpg`. Cela n'inclut pas la chaîne de requête ou les composants du fragment de l'URI. Pour plus d'informations, voir Uniform Resource Identifier (URI) : syntaxe générique.

À moins qu'une transformation ne soit spécifiée, un URI n'est pas normalisé et est inspecté au moment AWS où il est reçu du client dans le cadre de la demande. Une Transformation reformate l'URI comme spécifié.

Corps de texte

La partie d'une requête qui contient les données supplémentaires que vous souhaitez envoyer à votre serveur web en tant que corps de la requête HTTP, telles que les données d'un formulaire.

Paramètre de requête unique (valeur uniquement)

Tous les paramètres que vous avez définis dans le cadre de la chaîne de requête. Par exemple, si l'URL est « www.xyz.com ? UserName =abc& SalesRegion =seattle », vous pouvez ajouter un filtre au paramètre or. UserNameSalesRegion

Si vous choisissez Single query parameter (value only) (Paramètre de requête unique (valeur uniquement)), vous spécifierez également un Query parameter name (Nom du paramètre de requête). Il s'agit du paramètre de la chaîne de requête que vous allez inspecter, tel que UserName. La longueur maximale de Query parameter name (Nom du paramètre de requête) est de 30 caractères. Query parameter name (Nom du paramètre de requête) n'est pas sensible à la casse. Par exemple, si vous spécifiez le UserNamenom du paramètre Query, celui-ci correspondra à toutes les variantes de UserName, telles que username et UserName.

Tous les paramètres de requête (valeurs uniquement)

Semblable au paramètre de requête unique (valeur uniquement), mais plutôt que d'inspecter la valeur d'un seul paramètre, AWS WAF Classic inspecte les valeurs de tous les paramètres de la chaîne de requête pour détecter la contrainte de taille. Par exemple, si l'URL est « www.xyz.com ? UserName =abc& SalesRegion =seattle » et que vous choisissez Tous les paramètres de requête (valeurs uniquement), AWS WAF Classic déclenchera une correspondance dont la valeur est égale ou supérieure à la taille spécifiée. UserNameSalesRegion

En-tête (uniquement lorsque « Part of the request to filter on » est défini sur « Header »)

Si vous avez choisi En-tête pour une partie de la demande à filtrer, choisissez un en-tête dans la liste des en-têtes courants ou tapez le nom d'un en-tête dont vous souhaitez que AWS WAF Classic évalue la longueur.

Opérateur de comparaison

Choisissez la manière dont vous souhaitez que AWS WAF Classic évalue la longueur de la chaîne de requête dans les requêtes Web par rapport à la valeur que vous spécifiez pour Size.

Par exemple, si vous choisissez Is superior than pour l'opérateur de comparaison et tapez 100 pour Size, AWS WAF Classic évalue les demandes Web pour une chaîne de requête de plus de 100 octets.

Size

Entrez la longueur, en octets, que vous souhaitez que AWS WAF Classic surveille dans les chaînes de requête.

> **Note**
>
> Si vous choisissez URI comme valeur de Part of the request to filter on, / dans l'URI est comptabilisé comme un caractère. Par exemple, le chemin `/logo.jpg` de l'URI comporte neuf caractères.

Transformation

Une transformation reformate une requête Web avant que AWS WAF Classic n'évalue la longueur de la partie spécifiée de la demande. Cela élimine une partie du formatage inhabituel utilisé par les attaquants dans les requêtes Web dans le but de contourner AWS WAF Classic.

> **Note**
>
> Si vous choisissez Body for Part of the request à filtrer, vous ne pouvez pas configurer AWS WAF Classic pour effectuer une transformation car seuls les 8192 premiers octets sont transférés pour inspection. Cependant, vous pouvez toujours filtrer votre trafic en fonction de la taille du corps de la requête HTTP et spécifier une transformation égale à None. (AWS WAF Classic obtient la longueur du corps à partir des en-têtes de requête.)

Vous ne pouvez spécifier qu'un seul type de transformation de texte.

Les transformations peuvent effectuer les opérations suivantes :

Aucun

AWS WAF Classic n'effectue aucune transformation de texte sur la requête Web avant d'en vérifier la longueur.

Convertir en minuscules

AWS WAF Classic convertit les lettres majuscules (A-Z) en minuscules (a-z).

Décodage d'HTML

AWS WAF Classic remplace les caractères codés en HTML par des caractères non codés :

- Remplace `"` par &
- Remplace ` ` par un espace insécable
- Remplace `<` par <
- Remplace `>` par >
- Remplace les caractères qui sont représentées au format hexadécimal, `&#xhhhh;`, par les caractères correspondants
- Remplace les caractères qui sont représentés au format décimal, `&#nnnn;`, par les caractères correspondants

Normalisation des espaces blancs

AWS WAF Classic remplace les caractères suivants par un espace (32 décimal) :

- \f, saut de page, décimale 12
- \t, tabulation, décimale 9
- \n, nouvelle ligne, décimale 10
- \r, retour chariot, décimale 13
- \v, tabulation verticale, décimale 11
- Espace insécable, décimale 160

En outre, cette option remplace plusieurs espaces par un seul.

Simplifier la ligne de commande

Pour les requêtes qui contiennent des commandes de ligne de commande du système d'exploitation, utilisez cette option pour effectuer les transformations suivantes :

- Supprimer les caractères suivants : \ " ' ^
- Supprimer les espaces avant les caractères suivants : / (
- Remplacer les caractères suivants par un espace : , ;
- Remplacer plusieurs espaces par un espace
- Convertit les lettres majuscules (A-Z) en lettres minuscules (a-z)

Décodage d'URL

Décoder une requête encodée par URL.

Ajout et suppression de filtres dans une condition de contrainte de taille

Vous pouvez ajouter ou supprimer des filtres dans une condition de contrainte de taille. Pour modifier un filtre, ajoutez un nouveau filtre et supprimez l'ancien.

Pour ajouter ou supprimer des filtres d'une condition de contrainte de taille

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez Size constraint.
3. Sélectionnez la condition pour laquelle vous souhaitez ajouter ou supprimer des filtres.
4. Pour ajouter des filtres, effectuez les opérations suivantes :

   a. Choisissez Add filter.

   b. Indiquez les paramètres de filtre applicables. Pour plus d’informations, consultez Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de contrainte de taille.

   c. Choisissez Ajouter.
5. Pour supprimer des filtres, effectuez les opérations suivantes :

   a. Sélectionnez le filtre à supprimer.

   b. Choisissez Delete filter.

Suppression des conditions de contrainte de taille

Si vous souhaitez supprimer une condition de contrainte de taille, vous devez d'abord supprimer tous les filtres de la condition, puis supprimer la condition de toutes les règles qui l'utilisent, comme décrit dans la procédure suivante.

Pour supprimer une condition de contrainte de taille

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez Size constraints.
3. Dans le volet Size constraint conditions, sélectionnez la condition de contrainte de taille que vous souhaitez supprimer.
4. Dans le volet droit, choisissez l'onglet Associated rules.

   Si la liste des règles utilisant cette condition de contrainte de taille est vide, passez à l'étape 6. Si la liste contient une ou des règles, notez-les et passez à l'étape 5.
5. Pour supprimer la condition de contrainte de taille des règles qui l'utilisent, effectuez les opérations suivantes :

   a. Dans le volet de navigation, choisissez Règles.

   b. Choisissez le nom d'une règle qui utilise la condition de contrainte de taille que vous souhaitez supprimer.

   c. Dans le volet droit, sélectionnez la condition de contrainte de taille que vous souhaitez supprimer de la règle, puis sélectionnez Remove selected condition.

   d. Répétez les étapes b et c pour toutes les autres règles qui utilisent la condition de contrainte de taille que vous souhaitez supprimer.

   e. Dans le volet de navigation, choisissez Size constraint.

   f. Dans le volet Size constraint conditions, sélectionnez la condition de contrainte de taille que vous souhaitez supprimer.
6. Choisissez Delete pour supprimer la condition sélectionnée.

Utilisation des conditions de correspondance d'injection SQL

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Les pirates insèrent parfois du code SQL malveillant dans les requêtes web dans le but d'extraire des données de votre base de données. Pour autoriser ou bloquer des requêtes web qui semblent contenir du code SQL malveillant, créez une ou plusieurs conditions de correspondance d'injection SQL. Une condition de correspondance par injection SQL identifie la partie des requêtes Web, telle que le chemin de l'URI ou la chaîne de requête, que AWS WAF Classic doit inspecter. Ultérieurement dans le processus, lorsque vous créez une liste ACL web, vous spécifiez s'il convient d'autoriser ou de bloquer des requêtes qui semblent contenir du code SQL malveillant.

Rubriques

Création de conditions de correspondance d'injection SQL

Lorsque vous créez des conditions de correspondance par injection SQL, vous spécifiez des filtres qui indiquent la partie des requêtes Web que AWS WAF Classic doit inspecter pour détecter la présence de code SQL malveillant, telle que l'URI ou la chaîne de requête. Vous pouvez ajouter plus d'un filtre à une condition de correspondance d'injection SQL ou vous pouvez créer une condition distincte pour chaque filtre. Voici comment chaque configuration affecte le comportement AWS WAF classique :

- Plusieurs filtres par condition de correspondance par injection SQL (recommandé) — Lorsque vous ajoutez une condition de correspondance par injection SQL contenant plusieurs filtres à une règle et que vous ajoutez la règle à une ACL Web, il suffit qu'une requête Web corresponde à l'un des filtres de la condition de correspondance par injection SQL pour que AWS WAF Classic autorise ou bloque la demande en fonction de cette condition.

  Par exemple, supposons que vous créez une condition de correspondance d'injection SQL et que la condition contient deux filtres. Un filtre demande à AWS WAF Classic d'inspecter l'URI pour détecter la présence de code SQL malveillant, et l'autre indique à AWS WAF Classic d'inspecter la chaîne de requête. AWS WAF Classic autorise ou bloque les demandes si elles semblent contenir du code SQL malveillant dans l'URI ou dans la chaîne de requête.
- Un filtre par condition de correspondance d'injection SQL — Lorsque vous ajoutez les conditions de correspondance d'injection SQL distinctes à une règle et que vous ajoutez la règle à une ACL Web, les requêtes Web doivent répondre à toutes les conditions pour que AWS WAF Classic autorise ou bloque les demandes en fonction de ces conditions.

  Supposons que vous créez deux conditions et que chaque condition contient l'un des deux filtres de l'exemple précédent. Lorsque vous ajoutez les deux conditions à la même règle et que vous ajoutez la règle à une ACL Web, AWS WAF Classic autorise ou bloque les demandes uniquement lorsque l'URI et la chaîne de requête semblent contenir du code SQL malveillant.

> **Note**
>
> Lorsque vous ajoutez une condition de correspondance par injection SQL à une règle, vous pouvez également configurer AWS WAF Classic pour autoriser ou bloquer les requêtes Web qui ne semblent pas contenir de code SQL malveillant.

Pour créer une condition de correspondance d'injection SQL

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si vous voyez Passer à la AWS WAF version classique dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez SQL injection.
3. Choisissez Create condition.

4. Indiquez les paramètres de filtre applicables. Pour plus d'informations, consultez Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de correspondance d'injection SQL.
5. Choisissez Add another filter.
6. Si vous souhaitez ajouter un autre filtre, répétez les étapes 4 et 5.
7. Lorsque vous avez fini d'ajouter les filtres, choisissez Create.

Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de correspondance d'injection SQL

Lorsque vous créez ou mettez à jour une condition de correspondance d'injection SQL, vous spécifiez les valeurs suivantes :

Nom

Le nom de la condition de correspondance d'injection SQL.

Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./. Vous ne pouvez pas modifier la nom d'une condition après l'avoir créée.

Partie de la requête à filtrer

Choisissez la partie de chaque requête Web que AWS WAF Classic doit inspecter pour détecter la présence de code SQL malveillant :

En-tête

Un en-tête de requête spécifié, par exemple, l'en-tête `User-Agent` ou `Referer`. Si vous choisissez Header, précisez le nom de l'en-tête dans le champs Header.

Méthode HTTP

La méthode HTTP, qui indique le type d'opération que la demande demande à l'origine d'effectuer. CloudFront prend en charge les méthodes suivantes : `DELETEGET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, et`PUT`.

Chaîne de requête

La partie d'une URL qui s'affiche après un caractère ?, le cas échéant.

> **Note**
>
> Pour les conditions de correspondance d'injection SQL, nous vous recommandons de choisir All query parameters (values only) [Tous les paramètres de requête (valeurs uniquement)] au lieu de Query string (Chaîne de requête) pour Part of the request to filter on (Partie de la requête sur laquelle filtrer).

URI

Le chemin URI de la demande, qui identifie la ressource, par exemple,`/images/daily-ad.jpg`. Cela n'inclut pas la chaîne de requête ou les composants du fragment de l'URI. Pour plus d'informations, voir Uniform Resource Identifier (URI) : syntaxe générique.

À moins qu'une transformation ne soit spécifiée, un URI n'est pas normalisé et est inspecté au moment AWS où il est reçu du client dans le cadre de la demande. Une Transformation reformate l'URI comme spécifié.

Corps de texte

La partie d'une requête qui contient les données supplémentaires que vous souhaitez envoyer à votre serveur web en tant que corps de la requête HTTP, telles que les données d'un formulaire.

> **Note**
>
> Si vous choisissez Body pour la valeur d'une partie de la demande à filtrer, AWS WAF Classic inspecte uniquement les 8 192 premiers octets (8 Ko). Pour autoriser ou bloquer les demandes dont le corps est supérieur à 8 192 octets, vous pouvez créer une condition de contrainte de taille. (AWS WAF Classic obtient la longueur du corps à partir des en-têtes de requête.) Pour plus d'informations, consultez Utilisation des conditions de contrainte de taille.

Paramètre de requête unique (valeur uniquement)

Tous les paramètres que vous avez définis dans le cadre de la chaîne de requête. Par exemple, si l'URL est « www.xyz.com ? UserName =abc& SalesRegion =seattle », vous pouvez ajouter un filtre au paramètre or. UserNameSalesRegion

Si vous choisissez Single query parameter (value only) (Paramètre de requête unique (valeur uniquement)), vous spécifierez également un Query parameter name (Nom du paramètre de requête). Il s'agit du paramètre de la chaîne de requête que vous allez inspecter, tel que UserNameou SalesRegion. La longueur maximale de Query parameter name (Nom du paramètre de requête) est de 30 caractères. Query parameter name (Nom du paramètre de requête) n'est pas sensible à la casse. Par exemple, si vous spécifiez le UserNamenom du paramètre Query, celui-ci correspondra à toutes les variantes de UserName, telles que username et UserName.

Tous les paramètres de requête (valeurs uniquement)

Semblable au paramètre de requête unique (valeur uniquement), mais plutôt que d'inspecter la valeur d'un seul paramètre, AWS WAF Classic inspecte la valeur de tous les paramètres de la chaîne de requête pour détecter d'éventuels codes SQL malveillants. Par exemple, si l'URL est « www.xyz.com ? UserName =abc& SalesRegion =seattle » et que vous choisissez Tous les paramètres de requête (valeurs uniquement), AWS WAF Classic déclenchera une correspondance si la valeur de l'un ou UserNamel'autre contient un éventuel code SQL malveillant. SalesRegion

En-tête

Si vous avez choisi En-tête pour une partie de la demande à filtrer, choisissez un en-tête dans la liste des en-têtes courants ou entrez le nom d'un en-tête que AWS WAF Classic doit inspecter pour détecter la présence de code SQL malveillant.

Transformation

Une transformation reformate une requête Web avant que AWS WAF Classic ne l'inspecte. Cela élimine une partie du formatage inhabituel utilisé par les attaquants dans les requêtes Web dans le but de contourner AWS WAF Classic.

Vous ne pouvez spécifier qu'un seul type de transformation de texte.

Les transformations peuvent effectuer les opérations suivantes :

Aucun

AWS WAF Classic n'effectue aucune transformation de texte sur la requête Web avant de l'inspecter pour détecter la correspondance de la chaîne dans Value.

Convertir en minuscules

AWS WAF Classic convertit les lettres majuscules (A-Z) en minuscules (a-z).

Décodage d'HTML

AWS WAF Classic remplace les caractères codés en HTML par des caractères non codés :

- Remplace `"` par &
- Remplace ` ` par un espace insécable
- Remplace `<` par <
- Remplace `>` par >
- Remplace les caractères qui sont représentées au format hexadécimal, `&#xhhhh;`, par les caractères correspondants
- Remplace les caractères qui sont représentés au format décimal, `&#nnnn;`, par les caractères correspondants

Normalisation des espaces blancs

AWS WAF Classic remplace les caractères suivants par un espace (32 décimal) :

- \f, saut de page, décimale 12
- \t, tabulation, décimale 9
- \n, nouvelle ligne, décimale 10
- \r, retour chariot, décimale 13
- \v, tabulation verticale, décimale 11
- Espace insécable, décimale 160

En outre, cette option remplace plusieurs espaces par un seul.

Simplifier la ligne de commande

Pour les requêtes qui contiennent des commandes de ligne de commande du système d'exploitation, utilisez cette option pour effectuer les transformations suivantes :

- Supprimer les caractères suivants : \ " ' ^
- Supprimer les espaces avant les caractères suivants : / (
- Remplacer les caractères suivants par un espace : , ;
- Remplacer plusieurs espaces par un espace
- Convertit les lettres majuscules (A-Z) en lettres minuscules (a-z)

Décodage d'URL

Décoder une requête encodée par URL.

Ajout et suppression de filtres dans une condition de correspondance d'injection SQL

Vous pouvez ajouter ou supprimer des filtres dans une condition de correspondance d'injection SQL. Pour modifier un filtre, ajoutez un nouveau filtre et supprimez l'ancien.

Pour ajouter ou supprimer des filtres dans une condition de correspondance d'injection SQL

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si vous voyez Passer à la AWS WAF version classique dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez SQL injection.
3. Sélectionnez la condition pour laquelle vous souhaitez ajouter ou supprimer des filtres.
4. Pour ajouter des filtres, effectuez les opérations suivantes :
   a. Choisissez Add filter.
   b. Indiquez les paramètres de filtre applicables. Pour plus d’informations, consultez Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de correspondance d'injection SQL.
   c. Choisissez Ajouter.
5. Pour supprimer des filtres, effectuez les opérations suivantes :
   a. Sélectionnez le filtre à supprimer.
   b. Choisissez Delete filter.

Suppression des conditions de correspondance d'injection SQL

Si vous souhaitez supprimer une condition de correspondance d'injection SQL, vous devez d'abord supprimer tous les filtres de la condition, puis supprimer la condition de toutes les règles qui l'utilisent, comme décrit dans la procédure suivante.

Pour supprimer une condition de correspondance d'injection SQL

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

Si vous voyez Passer à la AWS WAF version classique dans le volet de navigation, sélectionnez-le.

2. Dans le volet de navigation, choisissez SQL injection.
3. Dans le volet SQL injection match conditions, choisissez la condition de correspondance d'injection SQL que vous souhaitez supprimer.
4. Dans le volet droit, choisissez l'onglet Associated rules.

   Si la liste des règles utilisant cette condition de correspondance d'injection SQL est vide, passez à l'étape 6. Si la liste contient une ou des règles, notez-les et passez à l'étape 5.
5. Pour supprimer la condition de correspondance d'injection SQL des règles qui l'utilisent, effectuez les opérations suivantes :

   a. Dans le volet de navigation, choisissez Règles.
   b. Choisissez le nom d'une règle qui utilise la condition de correspondance d'injection SQL que vous souhaitez supprimer.
   c. Dans le volet droit, sélectionnez la condition de correspondance d'injection SQL que vous souhaitez supprimer de la règle, puis sélectionnez Remove selected condition.
   d. Répétez les étapes b et c pour toutes les autres règles qui utilisent la condition de correspondance d'injection SQL que vous souhaitez supprimer.
   e. Dans le volet de navigation, choisissez SQL injection.
   f. Dans le volet SQL injection match conditions, choisissez la condition de correspondance d'injection SQL que vous souhaitez supprimer.
6. Choisissez Delete pour supprimer la condition sélectionnée.

Utilisation des conditions de correspondance de chaîne

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Si vous souhaitez autoriser ou bloquer des requêtes web en fonction des chaînes qui apparaissent dans les requêtes, créez une ou plusieurs conditions de correspondance de chaîne. Une condition de correspondance de chaîne identifie la chaîne que vous souhaitez rechercher et la partie des requêtes Web, telle qu'un en-tête spécifié ou la chaîne de requête, que AWS WAF Classic doit inspecter pour détecter la chaîne. Ultérieurement dans le processus, lorsque vous créez une liste ACL web, vous spécifiez s'il convient d'autoriser ou de bloquer les requêtes qui contiennent la chaîne.

Rubriques

Création d'une condition de correspondance de chaîne

Lorsque vous créez des conditions de correspondance de chaîne, vous spécifiez des filtres qui identifient la chaîne que vous souhaitez rechercher et la partie des requêtes Web que AWS WAF Classic doit inspecter pour cette chaîne, telle que l'URI ou la chaîne de requête. Vous pouvez ajouter plus d'un filtre à une condition de correspondance de chaîne ou vous pouvez créer une condition de correspondance de chaîne distincte pour chaque filtre. Voici comment chaque configuration affecte le comportement AWS WAF classique :

- Un filtre par condition de correspondance de chaîne — Lorsque vous ajoutez des conditions de correspondance de chaîne distinctes à une règle et que vous ajoutez la règle à une ACL Web, les requêtes Web doivent répondre à toutes les conditions pour que AWS WAF Classic autorise ou bloque les demandes en fonction de ces conditions.

  Par exemple, supposons que vous créez deux conditions. Une correspond aux requêtes web qui contiennent la valeur `BadBot` dans l'en-tête `User-Agent`. L'autre correspond aux requêtes web qui contiennent la valeur `BadParameter` dans les chaînes de requête. Lorsque vous ajoutez les deux conditions à la même règle et que vous ajoutez la règle à une ACL Web, AWS WAF Classic autorise ou bloque les demandes uniquement lorsqu'elles contiennent les deux valeurs.
- Plusieurs filtres par condition de correspondance de chaîne : lorsque vous ajoutez une condition de correspondance de chaîne contenant plusieurs filtres à une règle et que vous ajoutez la règle à une ACL Web, il suffit qu'une demande Web corresponde à l'un des filtres de la condition de

correspondance de chaîne pour que AWS WAF Classic autorise ou bloque la demande en fonction d'une seule condition.

Supposons que vous créiez une condition au lieu de deux et que celle-ci contienne les deux mêmes filtres que dans l'exemple précédent. AWS WAF Classic autorise ou bloque les demandes si elles sont contenues `BadBot` dans l'`User-Agent`en-tête ou `BadParameter` dans la chaîne de requête.

> **Note**
>
> Lorsque vous ajoutez une condition de correspondance de chaîne à une règle, vous pouvez également configurer AWS WAF Classic pour autoriser ou bloquer les requêtes Web qui ne correspondent pas aux valeurs de la condition.

Pour créer une condition de correspondance de chaîne

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez String and regex matching.
3. Choisissez Create condition.
4. Indiquez les paramètres de filtre applicables. Pour plus d'informations, consultez Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de correspondance de chaîne.
5. Choisissez Add filter.
6. Si vous souhaitez ajouter un autre filtre, répétez les étapes 4 et 5.
7. Lorsque vous avez fini d'ajouter les filtres, choisissez Create.

Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de correspondance de chaîne

Lorsque vous créez ou mettez à jour une condition de correspondance de chaîne, vous spécifiez les valeurs suivantes :

Nom

Saisissez un nom pour la condition de correspondance de chaîne. Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./. Vous ne pouvez pas modifier la nom d'une condition après l'avoir créée.

Type

Choisissez String match.

Partie de la requête à filtrer

Choisissez la partie de chaque requête Web que AWS WAF Classic doit inspecter pour trouver la chaîne que vous spécifiez dans Value to match :

En-tête

Un en-tête de requête spécifié, par exemple, l'en-tête `User-Agent` ou `Referer`. Si vous choisissez Header, précisez le nom de l'en-tête dans le champs Header.

Méthode HTTP

La méthode HTTP, qui indique le type d'opération que la demande demande à l'origine d'effectuer. CloudFront prend en charge les méthodes suivantes : `DELETEGET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, et`PUT`.

Chaîne de requête

La partie d'une URL qui s'affiche après un caractère `?`, le cas échéant.

URI

Le chemin URI de la demande, qui identifie la ressource, par exemple,`/images/daily-ad.jpg`. Cela n'inclut pas la chaîne de requête ou les composants du fragment de l'URI. Pour plus d'informations, voir Uniform Resource Identifier (URI) : syntaxe générique.

À moins qu'une transformation ne soit spécifiée, un URI n'est pas normalisé et est inspecté au moment AWS où il est reçu du client dans le cadre de la demande. Une Transformation reformate l'URI comme spécifié.

Corps de texte

La partie d'une requête qui contient les données supplémentaires que vous souhaitez envoyer à votre serveur web en tant que corps de la requête HTTP, telles que les données d'un formulaire.

> **Note**
>
> Si vous choisissez Body pour la valeur d'une partie de la demande à filtrer, AWS WAF Classic inspecte uniquement les 8 192 premiers octets (8 Ko). Pour autoriser ou bloquer les demandes dont le corps est supérieur à 8 192 octets, vous pouvez créer une condition de contrainte de taille. (AWS WAF Classic obtient la longueur du corps à partir des en-têtes de requête.) Pour plus d'informations, consultez Utilisation des conditions de contrainte de taille.

Paramètre de requête unique (valeur uniquement)

Tous les paramètres que vous avez définis dans le cadre de la chaîne de requête. Par exemple, si l'URL est « www.xyz.com ? UserName =abc& SalesRegion =seattle », vous pouvez ajouter un filtre au paramètre or. UserNameSalesRegion

Si les paramètres dupliqués apparaissent dans la chaîne de requête, les valeurs sont évaluées en tant que « OU ». Autrement dit, n'importe quelle valeur déclenchera une correspondance. Par exemple, dans l'URL « www.xyz.com ? SalesRegion =boston& SalesRegion =seattle », « boston » ou « seattle » dans Value to match déclenchera une correspondance.

Si vous choisissez Single query parameter (value only) (Paramètre de requête unique (valeur uniquement)), vous spécifierez également un Query parameter name (Nom du paramètre de requête). Il s'agit du paramètre de la chaîne de requête que vous allez inspecter, tel que UserNameou SalesRegion. La longueur maximale de Query parameter name (Nom du paramètre de requête) est de 30 caractères. Query parameter name (Nom du paramètre de requête) n'est pas sensible à la casse. Par exemple, si vous spécifiez le UserNamenom du paramètre Query, celui-ci correspondra à toutes les variantes de UserName, telles que username et UserName.

Tous les paramètres de requête (valeurs uniquement)

Semblable au paramètre de requête unique (valeur uniquement), mais plutôt que d'inspecter la valeur d'un seul paramètre, AWS WAF Classic inspecte la valeur de tous les paramètres de la chaîne de requête pour trouver la valeur à correspondre. Par exemple, si l'URL est « www.xyz.com ? UserName =abc& SalesRegion =seattle » et que vous choisissez Tous les paramètres de requête (valeurs uniquement), AWS WAF Classic déclenchera une correspondance si la valeur de l'un UserNameou l'autre SalesRegionest spécifiée comme valeur à correspondre.

En-tête (uniquement lorsque « Part of the request to filter on » est défini sur « Header »)

Si vous avez choisi En-tête dans la partie de la demande à filtrer dans la liste, choisissez un en-tête dans la liste des en-têtes courants ou entrez le nom d'un en-tête que AWS WAF Classic doit inspecter.

Type de correspondance

Dans la partie de la demande que AWS WAF Classic doit inspecter, choisissez l'endroit où la chaîne dans Value to match doit apparaître pour correspondre à ce filtre :

Contains

La chaîne s'affiche n'importe où dans la partie spécifiée de la requête.

Contient les mots

La partie spécifiée de la requête web doit inclure Value to match et Value to match doit uniquement contenir des caractères alphanumériques ou de soulignement (A-Z, a-z, 0-9, ou _). En outre, Value to match doit être un mot, ce qui implique l'une des déclarations suivantes :

- Value to match correspond exactement à la valeur de la partie spécifiée de la requête web, telles que la valeur d'un en-tête.
- Value to match est au début de la partie spécifiée de la requête web et est suivi par un caractère autre qu'un caractère alphanumérique ou de soulignement (_), par exemple, `BadBot;`.
- Value to match est à la fin de la partie spécifiée de la requête web et est précédé d'un caractère autre qu'un caractère alphanumérique ou de soulignement (_), par exemple, `;BadBot`.
- Value to match est au milieu de la partie spécifiée de la requête web et est précédé et suivi de caractères autre que des caractères alphanumériques ou de soulignement (_), par exemple, `-BadBot;`.

Exactly matches

La chaîne et la valeur de la partie spécifiée de la requête sont identiques.

Starts with

La chaîne s'affiche au début de la partie spécifiée de la requête.

Se termine par

La chaîne s'affiche à la fin de la partie spécifiée de la requête.

Transformation

Une transformation reformate une requête Web avant que AWS WAF Classic ne l'inspecte. Cela élimine une partie du formatage inhabituel utilisé par les attaquants dans les requêtes Web dans le but de contourner AWS WAF Classic.

Vous ne pouvez spécifier qu'un seul type de transformation de texte.

Les transformations peuvent effectuer les opérations suivantes :

Aucun

AWS WAF Classic n'effectue aucune transformation de texte sur la requête Web avant de l'inspecter pour détecter la correspondance de la chaîne dans Value.

Convertir en minuscules

AWS WAF Classic convertit les lettres majuscules (A-Z) en minuscules (a-z).

Décodage d'HTML

AWS WAF Classic remplace les caractères codés en HTML par des caractères non codés :

- Remplace `"` par &
- Remplace ` ` par un espace insécable
- Remplace `<` par <
- Remplace `>` par >
- Remplace les caractères qui sont représentées au format hexadécimal, `&#xhhhh;`, par les caractères correspondants
- Remplace les caractères qui sont représentés au format décimal, `&#nnnn;`, par les caractères correspondants

Normalisation des espaces blancs

AWS WAF Classic remplace les caractères suivants par un espace (32 décimal) :

- \f, saut de page, décimale 12
- \t, tabulation, décimale 9
- \n, nouvelle ligne, décimale 10
- \r, retour chariot, décimale 13
- \v, tabulation verticale, décimale 11

- Espace insécable, décimale 160

En outre, cette option remplace plusieurs espaces par un seul.

Simplifier la ligne de commande

Lorsque vous êtes préoccupé par le fait que des pirates puissent injecter une commande de ligne de commande du système d'exploitation et utilisent un formatage inhabituel pour masquer l'ensemble ou une partie de la commande, utilisez cette option pour effectuer les transformations suivantes :

- Supprimer les caractères suivants : \ " ' ^
- Supprimer les espaces avant les caractères suivants : / (
- Remplacer les caractères suivants par un espace : , ;
- Remplacer plusieurs espaces par un espace
- Convertit les lettres majuscules (A-Z) en lettres minuscules (a-z)

Décodage d'URL

Décoder une requête encodée par URL.

La valeur est codée en base64

Si la valeur de Value to match est codée en base64, cochez cette case. Utilisez l'encodage base64 pour spécifier des caractères non-imprimables, tel que des tabulations et des sauts de ligne, que les pirates incluent dans leurs requêtes.

Value to match

Spécifiez la valeur que vous souhaitez que AWS WAF Classic recherche dans les requêtes Web. La longueur maximale est de 50 octets. Si vous affectez un encodage en base64 à la valeur, la longueur maximale de 50 octets s'applique à la valeur avant que vous ne l'encodiez.

Ajout et suppression de filtres dans une condition de correspondance de chaîne

Vous pouvez ajouter des filtres à une condition de correspondance de chaîne ou supprimer des filtres. Pour modifier un filtre, ajoutez un nouveau filtre et supprimez l'ancien.

Pour ajouter ou supprimer des filtres à une condition de correspondance de chaîne

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.

2. Dans le volet de navigation, sélectionnez String and regex matching.
3. Sélectionnez la condition pour laquelle vous souhaitez ajouter ou supprimer des filtres.
4. Pour ajouter des filtres, effectuez les opérations suivantes :

   a. Choisissez Add filter.

   b. Indiquez les paramètres de filtre applicables. Pour plus d'informations, consultez Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de correspondance de chaîne.

   c. Choisissez Ajouter.
5. Pour supprimer des filtres, effectuez les opérations suivantes :

   a. Sélectionnez le filtre à supprimer.

   b. Choisissez Delete Filter.

Suppression de conditions de correspondance de chaîne

Si vous souhaitez supprimer une condition de correspondance de chaîne, vous devez d'abord supprimer tous les filtres de la condition, puis supprimer la condition de toutes les règles qui l'utilisent, comme décrit dans la procédure suivante.

Pour supprimer une condition de correspondance de chaîne

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Supprimez la condition de correspondance de chaîne des règles qui l'utilisent :

   a. Dans le volet de navigation, choisissez Règles.

   b. Choisissez le nom d'une règle qui utilise la condition de correspondance de chaîne que vous souhaitez supprimer.

   c. Dans le volet droit, choisissez Edit rule.

   d. Choisissez le X en regard de la condition que vous voulez supprimer.

e. Choisissez Mettre à jour.

f. Répétez les étapes pour toutes les autres règles qui utilisent la condition de correspondance de chaîne que vous souhaitez supprimer.

3. Supprimez les filtres de la condition que vous voulez supprimer :

   a. Dans le volet de navigation, sélectionnez String and regex matching.

   b. Choisissez le nom de la condition de correspondance de chaîne que vous souhaitez supprimer.

   c. Dans le volet droit, cochez la case en regard de Filter pour sélectionner tous les filtres.

   d. Choisissez Delete Filter.

4. Dans le volet de navigation, sélectionnez String and regex matching.

5. Dans le volet String and regex match conditions, sélectionnez la condition de correspondance de chaîne que vous voulez supprimer.

6. Choisissez Delete pour supprimer la condition sélectionnée.

Utilisation des conditions de correspondance d'expression régulière

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Si vous souhaitez autoriser ou bloquer des demandes web basées sur les chaînes correspondant à un modèle d'expression régulière qui apparaissent dans les demandes, créez une ou plusieurs conditions de correspondance d'expression régulière. Une condition de correspondance regex est un type de condition de correspondance de chaîne qui identifie le modèle que vous souhaitez rechercher et la partie des requêtes Web, telle qu'un en-tête spécifié ou la chaîne de requête, que AWS WAF Classic doit inspecter pour détecter le modèle. Ultérieurement dans le processus, lorsque vous créez une liste ACL web, vous spécifiez s'il convient d'autoriser ou de bloquer les demandes qui contiennent le modèle.

Rubriques

Création d'une condition de correspondance d'expression régulière

Lorsque vous créez des conditions de correspondance d'expression régulière, vous spécifiez les ensembles de modèle qui identifient la chaîne (à l'aide d'une expression régulière) que vous souhaitez rechercher. Vous ajoutez ensuite ces ensembles de modèles aux filtres qui spécifient la partie des requêtes Web que AWS WAF Classic doit inspecter pour ce jeu de modèles, telle que l'URI ou la chaîne de requête.

Vous pouvez ajouter plusieurs expressions régulières à un seul ensemble de modèles. Dans ce cas, ces expressions sont associées avec un OR. Ainsi, une demande web correspond à l'ensemble des modèles si la partie appropriée de la demande correspond à l'une des expressions répertoriées.

Lorsque vous ajoutez une condition de correspondance regex à une règle, vous pouvez également configurer AWS WAF Classic pour autoriser ou bloquer les requêtes Web qui ne correspondent pas aux valeurs de la condition.

AWS WAF Classic prend en charge la plupart des expressions régulières compatibles Perl (PCRE) standard. Cependant, les éléments suivants ne sont pas pris en charge :

- Références arrières et capture de sous-expressions
- Assertions arbitraires de largeur zéro
- Références de sous-routines et modèles récursifs
- Modèles conditionnels
- Verbes de contrôle de suivi arrière
- Directive octet unique \C
- Directive de correspondance de nouvelle ligne \R
- Début \K de directive de réinitialisation de correspondance
- Légendes et code intégré
- Regroupement atomique et quantificateurs possessifs

Pour créer une condition de correspondance d'expression régulière

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez String and regex matching.
3. Choisissez Create condition.
4. Indiquez les paramètres de filtre applicables. Pour plus d'informations, consultez Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de RegEx correspondance.
5. Choisissez Create pattern set and add filter (si vous avez créé un nouvel ensemble de modèles) ou Add filter si vous avez utilisé un ensemble de modèles existant.
6. Choisissez Créer.

Valeurs que vous spécifiez lorsque vous créez ou modifiez des conditions de RegEx correspondance

Lorsque vous créez ou mettez à jour une condition de correspondance d'expression régulière, vous spécifiez les valeurs suivantes :

Nom

Saisissez un nom pour la condition de correspondance d'expression régulière. Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./. Vous ne pouvez pas modifier la nom d'une condition après l'avoir créée.

Type

Choisissez Regex match.

Partie de la requête à filtrer

Choisissez la partie de chaque requête Web que AWS WAF Classic doit inspecter pour déterminer le modèle que vous spécifiez dans Value to match :

En-tête

Un en-tête de requête spécifié, par exemple, l'en-tête `User-Agent` ou `Referer`. Si vous choisissez Header, précisez le nom de l'en-tête dans le champs Header.

Méthode HTTP

La méthode HTTP, qui indique le type d'opération que la demande demande à l'origine d'effectuer. CloudFront prend en charge les méthodes suivantes : `DELETEGET`,`HEAD`,`OPTIONS`,`PATCH`,`POST`, et`PUT`.

Chaîne de requête

La partie d'une URL qui s'affiche après un caractère `?`, le cas échéant.

URI

Le chemin URI de la demande, qui identifie la ressource, par exemple,`/images/daily-ad.jpg`. Cela n'inclut pas la chaîne de requête ou les composants du fragment de l'URI. Pour plus d'informations, voir Uniform Resource Identifier (URI) : syntaxe générique.

À moins qu'une transformation ne soit spécifiée, un URI n'est pas normalisé et est inspecté au moment AWS où il est reçu du client dans le cadre de la demande. Une Transformation reformate l'URI comme spécifié.

Corps de texte

La partie d'une requête qui contient les données supplémentaires que vous souhaitez envoyer à votre serveur web en tant que corps de la requête HTTP, telles que les données d'un formulaire.

> **Note**
>
> Si vous choisissez Body pour la valeur d'une partie de la demande à filtrer, AWS WAF Classic inspecte uniquement les 8 192 premiers octets (8 Ko). Pour autoriser ou bloquer les demandes dont le corps est supérieur à 8 192 octets, vous pouvez créer une condition de contrainte de taille. (AWS WAF Classic obtient la longueur du corps à partir des en-têtes de requête.) Pour plus d'informations, consultez Utilisation des conditions de contrainte de taille.

Paramètre de requête unique (valeur uniquement)

Tous les paramètres que vous avez définis dans le cadre de la chaîne de requête. Par exemple, si l'URL est « www.xyz.com ? UserName =abc& SalesRegion =seattle », vous pouvez ajouter un filtre au paramètre or. UserNameSalesRegion

Si les paramètres dupliqués apparaissent dans la chaîne de requête, les valeurs sont évaluées en tant que « OU ». Autrement dit, n'importe quelle valeur déclenchera une correspondance. Par exemple, dans l'URL « www.xyz.com ? SalesRegion =boston& SalesRegion =seattle », un modèle qui correspond à « boston » ou à « seattle » dans Value to match déclenchera une correspondance.

Si vous choisissez Single query parameter (value only) (Paramètre de requête unique (valeur uniquement)), vous spécifierez également un Query parameter name (Nom du paramètre de requête). Il s'agit du paramètre de la chaîne de requête que vous allez inspecter, tel que UserNameou SalesRegion. La longueur maximale de Query parameter name (Nom du paramètre de requête) est de 30 caractères. Query parameter name (Nom du paramètre de requête) n'est pas sensible à la casse. Par exemple, si vous spécifiez le UserNamenom du paramètre Query, celui-ci correspondra à toutes les variantes de UserName, telles que username et UserName.

Tous les paramètres de requête (valeurs uniquement)

Semblable au paramètre de requête unique (valeur uniquement), mais plutôt que d'inspecter la valeur d'un seul paramètre, AWS WAF Classic inspecte la valeur de tous les paramètres de la chaîne de requête afin de détecter le modèle spécifié dans la valeur à mettre en correspondance. Par exemple, dans l'URL « www.xyz.com ? UserName =abc& SalesRegion =seattle », un modèle dans Value to match qui correspond à la valeur contenue dans ou déclenchera une correspondance. UserNameSalesRegion

En-tête (uniquement lorsque « Part of the request to filter on » est défini sur « Header »)

Si vous avez choisi En-tête dans la partie de la demande à filtrer dans la liste, choisissez un en-tête dans la liste des en-têtes courants ou entrez le nom d'un en-tête que AWS WAF Classic doit inspecter.

Transformation

Une transformation reformate une requête Web avant que AWS WAF Classic ne l'inspecte. Cela élimine une partie du formatage inhabituel utilisé par les attaquants dans les requêtes Web dans le but de contourner AWS WAF Classic.

Vous ne pouvez spécifier qu'un seul type de transformation de texte.

Les transformations peuvent effectuer les opérations suivantes :

Aucun

AWS WAF Classic n'effectue aucune transformation de texte sur la requête Web avant de l'inspecter pour détecter la correspondance de la chaîne dans Value.

Convertir en minuscules

AWS WAF Classic convertit les lettres majuscules (A-Z) en minuscules (a-z).

Décodage d'HTML

AWS WAF Classic remplace les caractères codés en HTML par des caractères non codés :

- Remplace `"` par &
- Remplace ` ` par un espace insécable
- Remplace `<` par <
- Remplace `>` par >
- Remplace les caractères qui sont représentées au format hexadécimal, `&#xhhhh;`, par les caractères correspondants
- Remplace les caractères qui sont représentés au format décimal, `&#nnnn;`, par les caractères correspondants

Normalisation des espaces blancs

AWS WAF Classic remplace les caractères suivants par un espace (32 décimal) :

- \f, saut de page, décimale 12
- \t, tabulation, décimale 9
- \n, nouvelle ligne, décimale 10
- \r, retour chariot, décimale 13
- \v, tabulation verticale, décimale 11
- Espace insécable, décimale 160

En outre, cette option remplace plusieurs espaces par un seul.

Simplifier la ligne de commande

Lorsque vous êtes préoccupé par le fait que des pirates puissent injecter une commande de ligne de commande du système d'exploitation et utilisent un formatage inhabituel pour masquer l'ensemble ou une partie de la commande, utilisez cette option pour effectuer les transformations suivantes :

- Supprimer les caractères suivants : \ " ' ^
- Supprimer les espaces avant les caractères suivants : / (
- Remplacer les caractères suivants par un espace : , ;
- Remplacer plusieurs espaces par un espace
- Convertit les lettres majuscules (A-Z) en lettres minuscules (a-z)

Décodage d'URL

Décoder une requête encodée par URL.

Modèle d'expression régulière pour correspondre aux demandes

Vous pouvez choisir un ensemble de modèles existant ou en créer un. Si vous en créez un nouveau, spécifiez ce qui suit :

Nouveau nom d'ensemble de modèles

Entrez un nom, puis spécifiez le modèle d'expression régulière que vous souhaitez que AWS WAF Classic recherche.

Si vous ajoutez plusieurs expressions régulières à un ensemble de modèles, ces expressions sont associées avec un OR. Ainsi, une demande web correspond à l'ensemble des modèles si la partie appropriée de la demande correspond à l'une des expressions répertoriées.

La longueur maximale de Value to match est 70 caractères.

Modification d'une condition de correspondance d'expression régulière

Vous pouvez apporter les modifications suivantes à une condition de correspondance d'expression régulière existante :

- Supprimer un modèle à partir d'un ensemble de modèles existant
- Ajouter un modèle à un ensemble de modèles existant
- Supprimer un filtre d'une condition de correspondance d'expression régulière existante
- Ajoutez un filtre à une condition de correspondance regex existante (vous ne pouvez avoir qu'un seul filtre dans une condition de correspondance regex. Par conséquent, pour ajouter un filtre, vous devez d'abord supprimer le filtre existant.)
- Supprimer une condition de correspondance d'expression régulière existante

> **Note**
>
> Vous ne pouvez pas ajouter un ensemble de modèles à un filtre existant ou l'en supprimer. Vous devez modifier l'ensemble de modèles, ou supprimer le filtre et créer un nouveau filtre avec un nouvel ensemble de modèles.

Pour supprimer un modèle d'un ensemble de modèles existant

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez String and regex matching.
3. Choisissez View regex pattern sets.
4. Choisissez le nom de l'ensemble de modèles que vous voulez modifier.
5. Choisissez Modifier.
6. Choisissez le X en regard du modèle que vous voulez supprimer.
7. Choisissez Enregistrer.

Pour ajouter un modèle à un ensemble de modèles existant

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez String and regex matching.
3. Choisissez View regex pattern sets.
4. Choisissez le nom de l'ensemble de modèles à modifier.
5. Choisissez Modifier.
6. Saisissez un nouveau modèle d'expression régulière.
7. Choisissez le + en regard du nouveau modèle.

8. Choisissez Enregistrer.

Pour supprimer un filtre d'une condition de correspondance d'expression régulière existante

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez String and regex matching.
3. Choisissez le nom de la condition associée au filtre que vous souhaitez supprimer.
4. Cochez la case en regard du filtre que vous voulez supprimer.
5. Choisissez Delete filter.

Pour supprimer une condition de correspondance d'expression régulière

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Supprimez le filtre de la condition regex. Pour plus d'instructions, consultez Pour supprimer un filtre d'une condition de correspondance d'expression régulière existante.)
3. Supprimez la condition de correspondance d'expression régulière des règles qui l'utilisent :

   a. Dans le volet de navigation, choisissez Règles.

   b. Choisissez le nom d'une règle qui utilise la condition de correspondance d'expression régulière que vous souhaitez supprimer.

   c. Dans le volet droit, choisissez Edit rule.

   d. Choisissez le X en regard de la condition que vous voulez supprimer.

   e. Choisissez Mettre à jour.

   f. Répétez les étapes pour toutes les autres règles qui utilisent la condition de correspondance d'expression régulière que vous souhaitez supprimer.
4. Dans le volet de navigation, sélectionnez String and regex matching.
5. Sélectionnez le bouton en regard de la condition que vous voulez supprimer.

6. Sélectionnez Delete (Supprimer).

Pour ajouter un filtre à une condition de correspondance d'expression régulière existante ou le modifier

Vous pouvez n'avoir qu'un seul filtre dans une condition de correspondance d'expression régulière. Si vous souhaitez ajouter ou modifier le filtre, vous devez d'abord supprimer le filtre existant.

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Supprimez le filtre de la condition d'expression régulière que vous voulez modifier. Pour plus d'instructions, consultez Pour supprimer un filtre d'une condition de correspondance d'expression régulière existante.)
3. Dans le volet de navigation, sélectionnez String and regex matching.
4. Choisissez le nom de la condition que vous voulez modifier.
5. Choisissez Add filter.
6. Entrez les valeurs appropriées pour le nouveau filtre et choisissez Add.

Utilisation des règles

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Les règles vous permettent de cibler précisément les requêtes Web que AWS WAF Classic doit autoriser ou bloquer en spécifiant les conditions exactes que vous souhaitez que AWS WAF Classic surveille. Par exemple, AWS WAF Classic peut surveiller les adresses IP d'où proviennent les

demandes, les chaînes que les demandes contiennent et l'endroit où elles apparaissent, et si les demandes semblent contenir du code SQL malveillant.

Rubriques

Création d'une règle et ajout de conditions

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Si vous ajoutez plusieurs conditions à une règle, une demande Web doit répondre à toutes les conditions pour que AWS WAF Classic autorise ou bloque les demandes en fonction de cette règle.

Pour créer une règle et ajouter des conditions

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez Règles.
3. Choisissez Créer une règle.
4. Entrez les valeurs suivantes :

Nom

Entrez un nom.

CloudWatch nom de la métrique

Entrez le nom de la CloudWatch métrique que AWS WAF Classic créera et associera à la règle. Le nom peut uniquement contenir des caractères alphanumériques (A-Z, a-z, 0-9), avec une longueur maximale de 128 caractères et une longueur minimale d'un caractère. Il ne peut pas contenir d'espaces blancs ou de noms de métriques réservés à AWS WAF Classic, notamment « All » et « Default_Action ».

Type de règle

Choisissez `Regular rule` ou `Rate-based rule`. Les règles basées sur le débit sont identiques aux règles normales, mais elles tiennent également compte du nombre de demandes provenant d'une adresse IP sur une période de cinq minutes. Pour plus d'informations sur ces types de règle, consultez Comment fonctionne AWS WAF Classic.

Limite de débit

Pour une règle basée sur le débit, saisissez le nombre maximal de requêtes à autoriser par période de cinq minutes provenant d'une adresse IP correspondant aux conditions de la règle. La limite de débit doit être d'au moins 100.

Vous pouvez spécifier uniquement une limite de débit, ou une limite de débit et des conditions. Si vous spécifiez uniquement une limite de débit, AWS WAF place la limite sur toutes les adresses IP. Si vous spécifiez une limite de débit et des conditions, AWS WAF place la limite sur les adresses IP qui répondent à ces conditions.

Lorsqu'une adresse IP atteint le seuil limite de débit, AWS WAF applique l'action assignée (bloquer ou compter) le plus rapidement possible, généralement dans les 30 secondes. Une fois l'action en place, si cinq minutes s'écoulent sans qu'aucune demande ne soit envoyée par l'adresse IP, AWS WAF le compteur est remis à zéro.

5. Pour ajouter une condition à la règle, spécifiez les valeurs suivantes :

does/does not pour une requête

Si vous souhaitez que AWS WAF Classic autorise ou bloque les demandes en fonction des filtres d'une condition, sélectionnez Oui. Par exemple, si une condition de correspondance

IP inclut la plage d'adresses IP 192.0.2.0/24 et que vous souhaitez que AWS WAF Classic autorise ou bloque les demandes provenant de ces adresses IP, choisissez does.

Si vous souhaitez que AWS WAF Classic autorise ou bloque les demandes en fonction de l'inverse des filtres d'une condition, choisissez Non. Par exemple, si une condition de correspondance IP inclut la plage d'adresses IP 192.0.2.0/24 et que vous souhaitez que AWS WAF Classic autorise ou bloque les demandes qui ne proviennent pas de ces adresses IP, Choose does not.

match/originate from

Choisissez le type de condition que vous voulez ajouter à la règle :

- Conditions de correspondance des scripts intersites : choisissez de faire correspondre au moins un des filtres dans la condition de correspondance des scripts intersites
- Conditions de correspondance IP : choisissez l'origine à partir d'une adresse IP dans
- Conditions de correspondance géographique : choisissez l'origine à partir d'un emplacement géographique dans
- Conditions de contrainte de taille : choisissez de faire correspondre au moins un des filtres de la condition de contrainte de taille
- Conditions de correspondance par injection SQL : choisissez faire correspondre au moins un des filtres dans la condition de correspondance par injection SQL
- Conditions de correspondance de chaîne : choisissez de faire correspondre au moins un des filtres de la condition de correspondance de chaîne
- Conditions de correspondance des expressions régulières : choisissez faire correspondre au moins un des filtres de la condition de correspondance des expressions régulières

condition name

Choisissez la condition que vous souhaitez ajouter à la règle. La liste affiche uniquement les conditions du type que vous avez choisi à l'étape précédente.

6. Pour ajouter une autre condition à la règle, choisissez Add another condition, répétez les étapes 4 et 5. Notez ce qui suit :

- Si vous ajoutez plusieurs conditions, une requête Web doit correspondre à au moins un filtre dans chaque condition pour que AWS WAF Classic autorise ou bloque les demandes en fonction de cette règle

- Si vous ajoutez deux conditions de correspondance d'adresses IP à la même règle, AWS WAF Classic autorisera ou bloquera uniquement les demandes provenant d'adresses IP figurant dans les deux conditions de correspondance d'adresses IP

7. Lorsque vous avez fini d'ajouter les conditions, choisissez Create.

Ajout et suppression de conditions dans une règle

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Vous pouvez modifier une règle en ajoutant ou en supprimant des conditions.

Pour ajouter ou supprimer des conditions d'une règle

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez Règles.
3. Sélectionnez le nom de la règle dans laquelle vous souhaitez ajouter ou supprimer des conditions.
4. Choisissez Ajouter une règle.
5. Pour ajouter une condition, choisissez Add condition et spécifiez les valeurs suivantes :

   does/does not pour une requête

   Si vous souhaitez que AWS WAF Classic autorise ou bloque les demandes en fonction des filtres d'une condition, par exemple les demandes Web provenant de la plage d'adresses IP 192.0.2.0/24, choisissez does.

Si vous souhaitez que AWS WAF Classic autorise ou bloque les demandes en fonction de l'inverse des filtres d'une condition, choisissez Non. Par exemple, si une condition de correspondance IP inclut la plage d'adresses IP 192.0.2.0/24 et que vous souhaitez que AWS WAF Classic autorise ou bloque les demandes qui ne proviennent pas de ces adresses IP, Choose does not.

match/originate from

Choisissez le type de condition que vous voulez ajouter à la règle :

- Conditions de correspondance des scripts intersites : choisissez de faire correspondre au moins un des filtres dans la condition de correspondance des scripts intersites
- Conditions de correspondance IP : choisissez l'origine à partir d'une adresse IP dans
- Conditions de correspondance géographique : choisissez l'origine à partir d'un emplacement géographique dans
- Conditions de contrainte de taille : choisissez de faire correspondre au moins un des filtres de la condition de contrainte de taille
- Conditions de correspondance par injection SQL : choisissez faire correspondre au moins un des filtres dans la condition de correspondance par injection SQL
- Conditions de correspondance de chaîne : choisissez de faire correspondre au moins un des filtres de la condition de correspondance de chaîne
- Conditions de correspondance des expressions régulières : choisissez faire correspondre au moins un des filtres de la condition de correspondance des expressions régulières

condition name

Choisissez la condition que vous souhaitez ajouter à la règle. La liste affiche uniquement les conditions du type que vous avez choisi à l'étape précédente.

6. Pour supprimer une condition, sélectionnez le X à droite du nom de la condition
7. Choisissez Mettre à jour.

Suppression d'une règle

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS

WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
Pour la dernière version de AWS WAF, voirAWS WAF.

Si vous souhaitez supprimer une règle, vous devez d'abord supprimer la règle des listes ACL web qui l'utilisent, puis supprimer les conditions qui sont incluses dans la règle.

Pour supprimer une règle

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Pour supprimer la règle des ACL Web qui l'utilisent, effectuez les étapes suivantes pour chacune des ACL Web :

   a. Dans le volet de navigation, choisissez Web ACLs.

   b. Choisissez le nom d'une liste ACL web qui utilise la règle que vous souhaitez supprimer.

   c. Choisissez l'onglet Règles.

   d. Choisissez Edit web ACL.

   e. Choisissez le X à droite de la règle que vous souhaitez supprimer, puis choisissez Mettre à jour.
3. Dans le volet de navigation, choisissez Règles.
4. Sélectionnez le nom de la règle que vous voulez supprimer.
5. Sélectionnez Supprimer.

AWS Marketplace groupes de règles

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière

version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
Pour la dernière version de AWS WAF, voirAWS WAF.

AWS WAF Classic propose des groupes de AWS Marketplace règles pour vous aider à protéger vos ressources. AWS Marketplace les groupes de règles sont des ensembles de ready-to-use règles prédéfinies rédigées et mises à jour par AWS des entreprises AWS partenaires.

Certains groupes de AWS Marketplace règles sont conçus pour protéger des types spécifiques d'applications Web telles que WordPress Joomla ou PHP. D'autres groupes de AWS Marketplace règles offrent une protection étendue contre les menaces connues ou les vulnérabilités courantes des applications Web, telles que celles répertoriées dans le Top 10 de l'OWASP.

Vous pouvez installer un seul groupe de AWS Marketplace règles provenant de votre AWS partenaire préféré, et vous pouvez également ajouter vos propres règles AWS WAF classiques personnalisées pour une protection accrue. Si vous êtes soumis à des réglementations telles que les normes PCI ou HIPAA, vous pouvez peut-être utiliser des groupes de AWS Marketplace règles pour satisfaire aux exigences du pare-feu des applications Web.

AWS Marketplace les groupes de règles sont disponibles sans contrat à long terme et sans engagement minimum. Lorsque vous vous inscrivez à un groupe de règles, des frais mensuels (au prorata horaire) vous sont facturés, ainsi que des frais basés sur le volume de requêtes en cours. Pour plus d'informations, consultez la section Tarification AWS WAF classique et la description de chaque groupe de AWS Marketplace règles sur AWS Marketplace.

Mises à jour automatiques

Se tenir au courant de l'évolution constante du paysage des menaces peut s'avérer long et coûteux. AWS Marketplace les groupes de règles peuvent vous faire gagner du temps lorsque vous implémentez et utilisez AWS WAF Classic. Autre avantage : nos AWS partenaires mettent automatiquement à jour les groupes de AWS Marketplace règles lorsque de nouvelles vulnérabilités et menaces apparaissent. AWS

Un grand nombre de nos partenaires sont avertis en cas de nouvelles vulnérabilités avant que celles-ci ne soient divulguées publiquement. Ils peuvent mettre à jour les groupes de règles et les déployer avant même qu'une nouvelle menace ne soit largement connue. La plupart d'entre eux ont des équipes de recherche des menaces ayant pour mission d'enquêter et d'analyser les menaces les plus récentes afin de rédiger des règles des plus pertinentes.

Accès aux règles d'un groupe de AWS Marketplace règles

Chaque groupe de AWS Marketplace règles fournit une description complète des types d'attaques et de vulnérabilités contre lesquels il est conçu pour se protéger. Pour protéger la propriété intellectuelle des fournisseurs de groupes de règles, vous ne pouvez pas consulter les règles individuelles au sein d'un groupe de règles. Cette restriction permet également d'empêcher les utilisateurs malveillants de concevoir des menaces qui contournent les règles publiées.

Comme vous ne pouvez pas afficher les règles individuelles d'un groupe de AWS Marketplace règles, vous ne pouvez pas non plus modifier les règles d'un groupe de AWS Marketplace règles. En revanche, vous pouvez exclure des règles spécifiques d'un groupe de règles. Cela s'appelle une « exception de groupe de règles ». L'exclusion de règles ne supprime pas ces règles. Elle remplace simplement leur action par `COUNT`. Par conséquent, les requêtes qui correspondent à une règle exclue sont comptabilisées, mais ne sont pas bloquées. Vous recevez des métriques COUNT pour chaque règle exclue.

L'exclusion de règles peut être utile lors du dépannage de groupes de règles qui bloquent le trafic de manière inattendue (faux positifs). Une technique de dépannage consiste à identifier la règle spécifique au sein du groupe de règles qui bloque le trafic souhaité, puis à désactiver (exclure) cette règle.

En plus d'exclure des règles spécifiques, vous pouvez affiner votre protection en activant ou désactivant des groupes de règles complets, ainsi qu'en choisissant l'action de groupe de règles à exécuter. Pour plus d’informations, consultez Utilisation de groupes de AWS Marketplace règles.

Quotas

Vous ne pouvez activer qu'un seul groupe de AWS Marketplace règles. Vous pouvez également activer un groupe de règles personnalisé que vous créez à l'aide de AWS Firewall Manager. Ces groupes de règles comptent pour le quota maximal de 10 règles par liste ACL web. Par conséquent, vous pouvez avoir un groupe de AWS Marketplace règles, un groupe de règles personnalisées et jusqu'à huit règles personnalisées dans une seule ACL Web.

Tarification

Pour la tarification par groupe de AWS Marketplace règles, consultez la section Tarification AWS WAF classique et la description de chaque groupe de AWS Marketplace règles sur AWS Marketplace.

Utilisation de groupes de AWS Marketplace règles

Vous pouvez vous abonner à des groupes de AWS Marketplace règles et vous en désabonner sur la console AWS WAF Classic. Vous pouvez également exclure des règles spécifiques d'un groupe de règles.

Pour s'abonner à un groupe de AWS Marketplace règles et l'utiliser

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez Marketplace.
3. Dans la section Produits du Marketplace disponibles, choisissez le nom d'un groupe de règles pour afficher les détails et les informations de tarification.
4. Pour vous abonner au groupe de règles, choisissez Continuer.

   > **Note**
   >
   > Si vous ne souhaitez pas vous abonner à ce groupe de règles, fermez simplement cette page dans votre navigateur.
5. Choisissez Configurer votre compte.
6. Ajoutez le groupe de règles à une ACL Web, de la même manière que vous ajouteriez une règle individuelle. Pour plus d’informations, consultez Création d'une liste ACL web ou Modification d'une liste ACL web.

   > **Note**
   >
   > Lors de l'ajout d'un groupe de règles à une liste ACL web, l'action que vous définissez pour le groupe de règles (soit No override (Aucune substitution), soit Override to count (Substitution du nombre)) est appelée l'action de substitution du groupe de règles. Pour plus d’informations, consultez Substitution du groupe de règles.

Pour se désabonner d'un groupe de AWS Marketplace règles

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Supprimez le groupe de règles de toutes les ACL web. Pour plus d'informations, consultez Modification d'une liste ACL web.
3. Dans le volet de navigation, sélectionnez Marketplace.
4. Choisissez Manage your subscriptions.
5. Choisissez Annuler l'abonnement regard du nom du groupe de règles duquel vous souhaitez vous désabonner.
6. Choisissez Oui, annuler l'abonnement.

Pour exclure une règle d'un groupe de règles (exception de groupe de règles)

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Si ce n'est pas déjà fait, activez la journalisation AWS WAF classique. Pour plus d'informations, consultez Journalisation des informations de trafic de la liste ACL web. Utilisez les journaux AWS WAF classiques pour identifier les identifiants des règles que vous souhaitez exclure. Il s'agit en général de règles qui bloquent les requêtes légitimes.
3. Dans le volet de navigation, choisissez Web ACLs.
4. Choisissez le nom de la liste ACL web que vous voulez modifier. Cela ouvre une page contenant les détails de l'ACL Web dans le volet droit.

   > **Note**
   >
   > Le groupe de règles que vous voulez modifier doit être associé à une liste ACL web avant de pouvoir exclure une règle de ce groupe de règles.
5. Sous l'onglet Rules dans le volet droit, choisissez Edit web ACL.

6. Dans la section Rule group exceptions (Exceptions de groupe de règles), développez le groupe de règles à modifier.
7. Sélectionnez le X en regard de la règle que vous voulez exclure. Vous pouvez identifier l'identifiant de règle correct à l'aide des journaux AWS WAF classiques.
8. Choisissez Mettre à jour.

   L'exclusion de règles ne supprime pas ces règles du groupe de règles. Elle remplace simplement leur action par `COUNT`. Par conséquent, les requêtes qui correspondent à une règle exclue sont comptabilisées, mais ne sont pas bloquées. Vous recevez des métriques `COUNT` pour chaque règle exclue.

   > **Note**
   >
   > Vous pouvez utiliser cette même procédure pour exclure des règles de groupes de règles personnalisées que vous avez créés dans AWS Firewall Manager. Toutefois, plutôt que d'exclure une règle d'un groupe de règles personnalisé à l'aide de cette procédure, vous pouvez également modifier un groupe de règles personnalisé à l'aide de la procédure décrite dans Ajouter et supprimer des règles dans un groupe de règles AWS WAF classique.

Substitution du groupe de règles

AWS Marketplace les groupes de règles ont deux actions possibles : Aucune dérogation et Remplacer pour compter. Si vous souhaitez tester le groupe de règles, définissez l'action sur Substituer le nombre. Cette action de groupe de règles substituera donc toute action block spécifiée par des règles individuelles contenues dans le groupe. En d'autres termes, si l'action du groupe de règles est définie sur Substituer le nombre, au lieu de bloquer potentiellement les requêtes fondées sur l'action de règles individuelles dans le groupe, ces requêtes seront comptabilisées. À l'inverse, si vous définissez l'action du groupe de règles sur Aucune substitution, les actions des règles individuelles du groupe sont utilisées.

Dépannage des groupes de règles AWS Marketplace

Si vous constatez qu'un groupe de AWS Marketplace règles bloque le trafic légitime, effectuez les étapes suivantes.

Pour résoudre les problèmes d'un groupe de règles AWS Marketplace

1. Excluez les règles spécifiques qui bloquent le trafic légitime. Vous pouvez identifier quelles règles bloquent quelles demandes à l'aide des journaux AWS WAF classiques. Pour de plus amples informations sur l'exclusion de règles, veuillez consulter Pour exclure une règle d'un groupe de règles (exception de groupe de règles).
2. Si l'exclusion de règles spécifiques ne résout pas le problème, vous pouvez modifier l'action pour le groupe de AWS Marketplace règles de Aucune dérogation à Remplacer pour compter. La demande web peut ainsi passer, quelles que soient les actions des règles au sein du groupe de règles. Cela vous fournit également des CloudWatch statistiques Amazon pour le groupe de règles.
3. Après avoir défini l'action du groupe de AWS Marketplace règles sur Remplacer pour compter, contactez l'équipe d'assistance client du fournisseur du groupe de règles pour résoudre le problème de manière plus approfondie. Pour les coordonnées, consultez la liste du groupe de règles sur les pages de liste produit sur AWS Marketplace.

Contacter le service clientèle

En cas de problème avec AWS WAF Classic ou un groupe de règles géré par AWS, contactez AWS Support. En cas de problème avec un groupe de règles géré par un AWS partenaire, contactez l'équipe du support client de ce partenaire. Pour trouver les coordonnées des partenaires, consultez la liste des partenaires sur AWS Marketplace.

Création et vente de groupes de AWS Marketplace règles

Si vous souhaitez vendre des groupes de AWS Marketplace règles AWS Marketplace, consultez Comment vendre votre logiciel sur AWS Marketplace.

Utilisation des listes ACL web

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.

Pour la dernière version de AWS WAF, voirAWS WAF.

Lorsque vous ajoutez des règles à une ACL Web, vous spécifiez si vous souhaitez que AWS WAF Classic autorise ou bloque les demandes en fonction des conditions définies dans les règles. Si vous ajoutez plusieurs règles à une ACL Web, AWS WAF Classic évalue chaque demande par rapport aux règles dans l'ordre dans lequel vous les listez dans l'ACL Web. Lorsqu'une requête Web répond à toutes les conditions d'une règle, AWS WAF Classic prend immédiatement l'action correspondante (autoriser ou bloquer) et n'évalue pas la demande par rapport aux autres règles de l'ACL Web, le cas échéant.

Si une requête Web ne correspond à aucune des règles d'une ACL Web, AWS WAF Classic exécute l'action par défaut que vous avez spécifiée pour l'ACL Web. Pour plus d'informations, consultez Choix de l'action par défaut pour une liste ACL web.

Si vous souhaitez tester une règle avant de commencer à l'utiliser pour autoriser ou bloquer des demandes, vous pouvez configurer AWS WAF Classic pour compter les requêtes Web qui répondent aux conditions de la règle. Pour plus d'informations, voir Test des listes ACL web.

Rubriques

Choix de l'action par défaut pour une liste ACL web

Note

Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.

Pour la dernière version de AWS WAF, voirAWS WAF.

Lorsque vous créez et configurez une ACL Web, la première et la plus importante décision que vous devez prendre est de savoir si l'action par défaut doit être pour AWS WAF Classic d'autoriser les requêtes Web ou de bloquer les demandes Web. L'action par défaut indique ce que vous souhaitez que AWS WAF Classic fasse une fois qu'il a inspecté une requête Web pour toutes les conditions que vous spécifiez et que la demande Web ne répond à aucune de ces conditions :

- Autoriser : si vous souhaitez autoriser la plupart des utilisateurs à accéder à votre site Web, mais que vous souhaitez bloquer l'accès aux attaquants dont les demandes proviennent d'adresses IP spécifiées ou dont les demandes semblent contenir du code SQL malveillant ou des valeurs spécifiées, choisissez Autoriser comme action par défaut.
- Bloquer : si vous souhaitez empêcher la plupart des utilisateurs potentiels d'accéder à votre site Web, mais que vous souhaitez autoriser l'accès aux utilisateurs dont les demandes proviennent d'adresses IP spécifiées ou dont les demandes contiennent des valeurs spécifiques, choisissez Bloquer comme action par défaut.

De nombreuses décisions que vous prenez après avoir choisi une action par défaut dépendent si vous voulez autoriser ou bloquer la plupart des requêtes web. Par exemple, si vous souhaitez autoriser la plupart des requêtes, alors les conditions de correspondance que vous créez doivent généralement spécifier les requêtes web que vous souhaitez bloquer, comme les requêtes suivantes :

- Les requêtes provenant d'adresses IP qui effectuent un trop grand nombre de requêtes
- Demandes en provenance de pays dans lesquels vous n'avez pas d'activité ou qui sont la source d'attaques fréquentes
- Les requêtes qui incluent des valeurs fausses dans l'en-tête User-Agent
- Les requêtes qui semblent inclure du code SQL malveillant

Création d'une liste ACL web

Note

Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS

WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
Pour la dernière version de AWS WAF, voirAWS WAF.

Pour créer une liste ACL web

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.

2. Si c'est la première fois que vous utilisez AWS WAF Classic, choisissez Go to AWS WAF Classic, puis Configure Web ACL. Si vous avez déjà utilisé AWS WAF Classic, choisissez Web ACL dans le volet de navigation, puis choisissez Create Web ACL.
3. Pour le nom de l'ACL Web, entrez un nom.

   > **Note**
   >
   > Vous ne pouvez pas modifier le nom une fois que vous créez la liste ACL web.

4. Pour le nom de la CloudWatch métrique, modifiez le nom par défaut le cas échéant. Le nom peut uniquement contenir des caractères alphanumériques (A-Z, a-z, 0-9), avec une longueur maximale de 128 caractères et une longueur minimale d'un caractère. Il ne peut pas contenir d'espaces blancs ou de noms de métriques réservés à AWS WAF Classic, notamment « All » et « Default_Action ».

   > **Note**
   >
   > Vous ne pouvez pas modifier le nom une fois que vous créez la liste ACL web.

5. Choisissez une région dans Région .
6. Pour AWS resource, choisissez la ressource que vous souhaitez associer à cette liste ACL web, puis choisissez Next.
7. Si vous avez déjà créé les conditions que vous souhaitez que AWS WAF Classic utilise pour inspecter vos requêtes Web, choisissez Next, puis passez à l'étape suivante.

Si vous n'avez pas encore créé de conditions, faites-le maintenant. Pour plus d'informations, consultez les rubriques suivantes :

- Utilisation des conditions de correspondance de scripts inter-site
- Utilisation des conditions de correspondance IP
- Utilisation des conditions de correspondance géographique
- Utilisation des conditions de contrainte de taille
- Utilisation des conditions de correspondance d'injection SQL
- Utilisation des conditions de correspondance de chaîne
- Utilisation des conditions de correspondance d'expression régulière

8. Si vous avez déjà créé les règles ou les groupes de règles (ou si vous êtes abonné à un AWS Marketplace groupe de règles) que vous souhaitez ajouter à cette ACL Web, ajoutez-les à l'ACL Web :

   a. Dans la liste Rules, sélectionnez une règle.

   b. Choisissez Add rule to web ACL.

   c. Répétez les étapes a et b jusqu'à ce que vous ayez ajouté toutes les règles que vous souhaitez ajouter à cette liste ACL web.

   d. Passez à l'étape 10.

9. Si vous n'avez pas encore créé de règles, vous pouvez ajouter des règles maintenant :

   a. Choisissez Créer une règle.

   b. Entrez les valeurs suivantes :

      Nom

      Entrez un nom.

      CloudWatch nom de la métrique

      Entrez le nom de la CloudWatch métrique que AWS WAF Classic créera et associera à la règle. Le nom peut uniquement contenir des caractères alphanumériques (A-Z, a-z, 0-9), avec une longueur maximale de 128 caractères et une longueur minimale d'un caractère. Il ne peut pas contenir d'espaces blancs ou de noms de métriques réservés à AWS WAF Classic, notamment « All » et « Default_Action ».

> **Note**
>
> Vous ne pouvez pas modifier le nom de la métrique après avoir créé la règle.

c. Pour ajouter une condition à la règle, spécifiez les valeurs suivantes :

does/does not pour une requête

Si vous souhaitez que AWS WAF Classic autorise ou bloque les demandes en fonction des filtres d'une condition, par exemple les demandes Web provenant de la plage d'adresses IP 192.0.2.0/24, choisissez does.

Si vous souhaitez que AWS WAF Classic autorise ou bloque les demandes en fonction de l'inverse des filtres d'une condition, choisissez Non. Par exemple, si une condition de correspondance IP inclut la plage d'adresses IP 192.0.2.0/24 et que vous souhaitez que AWS WAF Classic autorise ou bloque les demandes qui ne proviennent pas de ces adresses IP, Choose does not.

match/originate from

Choisissez le type de condition que vous voulez ajouter à la règle :

- Conditions de correspondance des scripts intersites : choisissez de faire correspondre au moins un des filtres dans la condition de correspondance des scripts intersites
- Conditions de correspondance IP : choisissez l'origine à partir d'une adresse IP dans
- Conditions de correspondance géographique : choisissez l'origine à partir d'un emplacement géographique dans
- Conditions de contrainte de taille : choisissez de faire correspondre au moins un des filtres de la condition de contrainte de taille
- Conditions de correspondance par injection SQL : choisissez faire correspondre au moins un des filtres dans la condition de correspondance par injection SQL
- Conditions de correspondance de chaîne : choisissez de faire correspondre au moins un des filtres de la condition de correspondance de chaîne
- Conditions de correspondance regex : choisissez faire correspondre au moins un des filtres de la condition de correspondance regex

condition name

Choisissez la condition que vous souhaitez ajouter à la règle. La liste affiche uniquement les conditions du type que vous avez choisi dans la liste précédente.

d. Pour ajouter une autre condition à la règle, choisissez Add another condition, et répétez les étapes b et c. Notez ce qui suit :

- Si vous ajoutez plusieurs conditions, une requête Web doit correspondre à au moins un filtre dans chaque condition pour que AWS WAF Classic autorise ou bloque les demandes en fonction de cette règle.
- Si vous ajoutez deux conditions de correspondance d'adresses IP à la même règle, AWS WAF Classic autorisera ou bloquera uniquement les demandes provenant d'adresses IP figurant dans les deux conditions de correspondance d'adresses IP.

e. Répétez l'étape 9 jusqu'à ce que vous ayez créé toutes les règles que vous souhaitez ajouter à cette liste ACL web.

f. Choisissez Créer.

g. Continuez à l'étape 10.

10. Pour chaque règle ou groupe de règles de l'ACL Web, choisissez le type de gestion que vous souhaitez que AWS WAF Classic fournisse, comme suit :

- Pour chaque règle, choisissez si vous souhaitez que AWS WAF Classic autorise, bloque ou compte les requêtes Web en fonction des conditions de la règle :
  - Autoriser : API Gateway CloudFront ou Application Load Balancer répond avec l'objet demandé. Dans le cas où CloudFront, si l'objet ne se trouve pas dans le cache périphérique, CloudFront transmet la demande à l'origine.
  - Bloquer — API Gateway CloudFront ou Application Load Balancer répond à la demande avec un code d'état HTTP 403 (Interdit). CloudFront peut également répondre avec une page d'erreur personnalisée. Pour plus d'informations, consultez Utilisation de AWS WAF Classic avec des pages d'erreur CloudFront personnalisées.
  - Nombre — AWS WAF Classic incrémente un compteur de demandes qui répondent aux conditions de la règle, puis continue à inspecter la demande Web en fonction des règles restantes de l'ACL Web.

    Pour de plus amples informations sur l'utilisation de Count pour tester une liste ACL web avant de commencer à l'utiliser pour autoriser ou bloquer des demandes web, veuillez

consulter Comptabilisation des demandes web qui correspondent aux règles dans une liste ACL web.

- Pour chaque groupe de règles, définissez l'action de substitution pour le groupe de règles :
  - Aucune dérogation : entraîne l'utilisation des actions des règles individuelles au sein du groupe de règles.
  - Remplacer par décompte : remplace toutes les actions de blocage spécifiées par les règles individuelles du groupe, de sorte que toutes les demandes correspondantes sont uniquement prises en compte.

  Pour plus d'informations, consultez Substitution du groupe de règles.

11. Si vous souhaitez modifier l'ordre des règles dans l'ACL Web, utilisez les flèches de la colonne Ordre. AWS WAF Classic inspecte les requêtes Web en fonction de l'ordre dans lequel les règles apparaissent dans l'ACL Web.
12. Si vous souhaitez supprimer une règle que vous avez ajoutée à la liste ACL web, choisissez le x sur la ligne de la règle.
13. Choisissez l'action par défaut pour la liste ACL web. C'est l'action que AWS WAF Classic effectue lorsqu'une requête Web ne répond aux conditions d'aucune des règles de cette ACL Web. Pour plus d'informations, consultez Choix de l'action par défaut pour une liste ACL web.
14. Choisissez Review and create.
15. Vérifiez les paramètres de la liste ACL web, puis sélectionnez Confirm and create.

Associer ou dissocier une ACL Web à une API Amazon API Gateway, à une CloudFront distribution ou à un Application Load Balancer

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Pour associer ou dissocier une liste ACL web, exécutez la procédure applicable. Notez que vous pouvez également associer une ACL Web à une CloudFront distribution lorsque vous créez ou mettez à jour la distribution. Pour plus d'informations, consultez la section Utilisation de AWS WAF Classic pour contrôler l'accès à votre contenu dans le manuel Amazon CloudFront Developer Guide.

Les restrictions suivantes s'appliquent lors de l'association d'une liste ACL web :

- Chaque API API Gateway, Application Load Balancer et CloudFront distribution ne peuvent être associés qu'à une seule ACL Web.
- Les ACL Web associées à une CloudFront distribution ne peuvent pas être associées à un Application Load Balancer ou à une API API Gateway. L'ACL Web peut toutefois être associée à d'autres CloudFront distributions.

Pour associer une ACL Web à une API API Gateway, à une CloudFront distribution ou à un Application Load Balancer

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez Web ACLs.
3. Choisissez le nom de l'ACL Web que vous souhaitez associer à une API API Gateway, à une CloudFront distribution ou à un Application Load Balancer. Cela ouvre une page contenant les détails de l'ACL Web dans le volet droit.
4. Dans l'onglet Règles, sous AWS Ressources utilisant cette ACL Web, choisissez Ajouter une association.
5. Lorsque vous y êtes invité, utilisez la liste des ressources pour choisir l'API API Gateway, CloudFront la distribution ou l'Application Load Balancer auxquels vous souhaitez associer cette ACL Web. Si vous choisissez un Application Load Balancer, vous devez également spécifier une région.
6. Choisissez Ajouter.
7. Pour associer cette ACL Web à une API API Gateway supplémentaire, à une CloudFront distribution ou à un autre Application Load Balancer, répétez les étapes 4 à 6.

Pour dissocier une ACL Web d'une API API Gateway, d'une CloudFront distribution ou d'un Application Load Balancer

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez Web ACLs.
3. Choisissez le nom de l'ACL Web que vous souhaitez dissocier d'une API API Gateway, d'une CloudFront distribution ou d'un Application Load Balancer. Cela ouvre une page contenant les détails de l'ACL Web dans le volet droit.
4. Dans l'onglet Rules, sous AWS ressources utilisant cette ACL Web, choisissez le x pour chaque API API, CloudFront distribution ou Application Balancer d'API Gateway dont vous souhaitez dissocier cette ACL Web.

Modification d'une liste ACL web

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Pour ajouter ou supprimer des règles d'une liste ACL web ou modifier l'action par défaut, exécutez la procédure suivante.

Pour modifier une liste ACL web

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.

2. Dans le volet de navigation, choisissez Web ACLs.
3. Choisissez le nom de la liste ACL web que vous voulez modifier. Cela ouvre une page contenant les détails de l'ACL Web dans le volet droit.
4. Sous l'onglet Rules dans le volet droit, choisissez Edit web ACL.
5. Pour ajouter des règles à la liste ACL web, effectuez les opérations suivantes :
   a. Dans la liste Rules, sélectionnez la règle que vous souhaitez ajouter.
   b. Choisissez Add rule to web ACL.
   c. Répétez les étapes a et b jusqu'à ce que vous ayez ajouté toutes les règles souhaitées.
6. Si vous souhaitez modifier l'ordre des règles dans l'ACL Web, utilisez les flèches de la colonne Ordre. AWS WAF Classic inspecte les requêtes Web en fonction de l'ordre dans lequel les règles apparaissent dans l'ACL Web.
7. Pour supprimer une règle de la liste ACL web, choisissez x à droite de la ligne de cette règle. Cela ne supprime pas la règle de AWS WAF Classic, elle la supprime simplement de cette ACL Web.
8. Pour modifier l'action d'une règle ou de l'action par défaut pour la liste ACL web, sélectionnez l'option préférée.

   > **Note**
   >
   > Lorsque vous définissez l'action pour un groupe de règles ou un groupe de AWS Marketplace règles (par opposition à une seule règle), l'action que vous définissez pour le groupe de règles (Aucune dérogation ou Remplacer pour compter) est appelée action de dérogation. Pour plus d'informations, consultez Substitution du groupe de règles.

9. Sélectionnez Enregistrer les modifications.

Suppression d'une liste ACL web

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière

version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
Pour la dernière version de AWS WAF, voirAWS WAF.

Pour supprimer une ACL Web, vous devez supprimer les règles incluses dans l'ACL Web et dissocier toutes les CloudFront distributions et tous les équilibreurs de charge d'application de l'ACL Web. Utilisez la procédure suivante.

Supprimer une liste ACL web

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez Web ACLs.
3. Choisissez le nom de l'ACL Web que vous souhaitez supprimer. Cela ouvre une page contenant les détails de l'ACL Web dans le volet droit.
4. Sous l'onglet Rules dans le volet droit, choisissez Edit web ACL.
5. Pour supprimer toutes les règles de la liste ACL web, choisissez x à droite de la ligne de chaque règle. Cela ne supprime pas les règles de AWS WAF Classic, cela supprime simplement les règles de cette ACL Web.
6. Choisissez Mettre à jour.
7. Dissociez l'ACL Web de toutes les CloudFront distributions et de tous les équilibreurs de charge d'application. Dans l'onglet Rules, sous les AWS ressources utilisant cette ACL Web, choisissez le x pour chaque API API Gateway, CloudFront distribution ou Application Load Balancer.
8. Sur la page Web ACLs (Listes ACL web), confirmez que la liste ACL web que vous souhaitez supprimer est sélectionnée, puis choisissez Delete (Supprimer).

Test des listes ACL web

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS

WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
Pour la dernière version de AWS WAF, voirAWS WAF.

Pour vous assurer de ne pas configurer accidentellement AWS WAF Classic pour bloquer les requêtes Web que vous souhaitez autoriser ou autoriser les demandes que vous souhaitez bloquer, nous vous recommandons de tester minutieusement votre ACL Web avant de commencer à l'utiliser sur votre site Web ou votre application Web.

Rubriques

- Comptabilisation des demandes web qui correspondent aux règles dans une liste ACL web
- Affichage d'un échantillon des requêtes Web qu'API Gateway CloudFront ou un Application Load Balancer a transmises à Classic AWS WAF

Comptabilisation des demandes web qui correspondent aux règles dans une liste ACL web

Lorsque vous ajoutez des règles à une ACL Web, vous spécifiez si vous souhaitez que AWS WAF Classic autorise, bloque ou compte les requêtes Web qui répondent à toutes les conditions de cette règle. Nous vous recommandons de commencer par la configuration suivante :

- Configurer toutes les règles d'une liste ACL web pour compter les requêtes web
- Définir l'action par défaut pour que la liste ACL autorise les requêtes

Dans cette configuration, AWS WAF Classic inspecte chaque requête Web en fonction des conditions de la première règle. Si la requête Web répond à toutes les conditions de cette règle, AWS WAF Classic incrémente un compteur pour cette règle. AWS WAF Classic inspecte ensuite la requête Web en fonction des conditions de la règle suivante. Si la demande répond à toutes les conditions de cette règle, AWS WAF Classic incrémente un compteur pour la règle. Cela continue jusqu'à ce que AWS WAF Classic ait inspecté la demande en fonction des conditions de toutes vos règles.

Une fois que vous avez configuré toutes les règles d'une ACL Web pour compter les demandes et que vous avez associé l'ACL Web à une API Amazon API Gateway, à une CloudFront distribution ou à un Application Load Balancer, vous pouvez consulter les dénombrements obtenus dans un graphique Amazon CloudWatch. Pour chaque règle d'une ACL Web et pour toutes les demandes

qu'API Gateway CloudFront ou un Application Load Balancer transmet à AWS WAF Classic pour une ACL Web, vous pouvez CloudWatch :

- d'afficher les données de la dernière heure ou des trois dernières heures ;
- de modifier l'intervalle entre les points de données ;
- Modifier le calcul effectué sur CloudWatch les données, tel que le maximum, le minimum, la moyenne ou la somme

> **Note**
>
> AWS WAF Classic with CloudFront est un service mondial et les statistiques ne sont disponibles que lorsque vous choisissez la région USA Est (Virginie du Nord) dans le AWS Management Console. Si vous choisissez une autre région, aucune métrique AWS WAF classique n'apparaîtra dans la CloudWatch console.

Pour afficher les données des règles d'une liste ACL web

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation, sous Metrics, choisissez WAF.
3. Cochez la case de la liste ACL web dont vous voulez afficher les données.
4. Modifiez les paramètres applicables :

   Statistique

   Choisissez le calcul à CloudWatch effectuer sur les données.

   Plage horaire

   Choisissez si vous souhaitez afficher les données de la dernière heure ou des trois dernières heures.

   Période

   Choisissez l'intervalle entre les points de données sur le graphique.

   Règles

   Choisissez les règles dont vous souhaitez afficher les données.

Notez ce qui suit :

- Si vous venez d'associer une ACL Web à une API API Gateway, à une CloudFront distribution ou à un Application Load Balancer, vous devrez peut-être attendre quelques minutes pour que les données apparaissent dans le graphique et que la métrique de l'ACL Web apparaisse dans la liste des métriques disponibles.
- Si vous associez plusieurs API API Gateway, CloudFront distributions ou Application Load Balancer à une ACL Web, les CloudWatch données incluront toutes les demandes pour toutes les distributions associées à l'ACL Web.
- Vous pouvez passer le curseur de la souris sur un point de données pour obtenir plus d'informations.
- Le graphique n'est pas actualisé automatiquement. Pour mettre à jour l'affichage, cliquez sur l'icône
  ( ).

5. (Facultatif) Affichez des informations détaillées sur les demandes individuelles qu'API Gateway CloudFront ou un Application Load Balancer a transmises à AWS WAF Classic. Pour plus d'informations, consultez Affichage d'un échantillon des requêtes Web qu'API Gateway CloudFront ou un Application Load Balancer a transmises à Classic AWS WAF.
6. Si vous déterminez qu'une règle intercepte des requêtes que vous ne voulez pas qu'elle intercepte, modifiez les paramètres applicables. Pour plus d'informations, consultez Création et configuration d'une liste de contrôle d'accès web (liste ACL web).

   Lorsque vous êtes satisfait que toutes vos règles interceptent uniquement les bonnes requêtes, définissez l'action pour chacune de vos règles sur Allow ou Block. Pour plus d'informations, consultez Modification d'une liste ACL web.

Affichage d'un échantillon des requêtes Web qu'API Gateway CloudFront ou un Application Load Balancer a transmises à Classic AWS WAF

Dans la console AWS WAF Classic, vous pouvez consulter un échantillon des demandes qu'API Gateway CloudFront ou un Application Load Balancer a transmises à AWS WAF Classic pour inspection. Pour chaque exemple de requête, vous pouvez afficher des données détaillées sur la requête, telles que l'adresse IP d'origine et les en-têtes inclus dans la requête. Vous pouvez aussi afficher la règle à laquelle correspondait la requête, et si la règle est configurée pour autoriser ou bloquer des requêtes.

L'exemple de requêtes contient jusqu'à 100 demandes qui correspondaient à toutes les conditions de chaque règle et 100 autres demandes pour l'action par défaut, qui s'applique aux demandes qui ne correspondaient pas à toutes les conditions d'une règle. Les demandes présentées dans l'exemple proviennent de toutes les API API Gateway, de tous les sites CloudFront périphériques ou de tous les équilibreurs de charge d'application qui ont reçu des demandes concernant votre contenu au cours des 15 dernières minutes.

Pour consulter un échantillon des requêtes Web qu'API Gateway CloudFront ou un Application Load Balancer a transmises à Classic AWS WAF

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, sélectionnez la liste ACL web dont vous souhaitez afficher les requêtes.
3. Dans le volet droit, choisissez l'onglet Requests.

   Le tableau Sampled requests affiche les valeurs suivantes pour chaque requête :

   IP Source

   Soit l'adresse IP d'origine de la demande, soit, si le lecteur a utilisé un proxy HTTP ou un Application Load Balancer pour envoyer la demande, l'adresse IP du proxy ou de l'Application Load Balancer.

   URI

   Le chemin URI de la demande, qui identifie la ressource, par exemple,`/images/daily-ad.jpg`. Cela n'inclut pas la chaîne de requête ou les composants du fragment de l'URI. Pour plus d'informations, voir Uniform Resource Identifier (URI) : syntaxe générique.

   Correspond à la règle

   Identifie la première règle dans la liste ACL web pour laquelle la requête web correspondait à toutes les conditions. Si une requête web ne correspond pas à toutes les conditions d'une règle dans la liste ACL web, la valeur de Matches rule est Default.

   Notez que lorsqu'une requête Web répond à toutes les conditions d'une règle et que l'action correspondant à cette règle est Count, AWS WAF Classic continue d'inspecter la demande

Web en fonction des règles suivantes de l'ACL Web. Dans ce cas, une requête web peut apparaître deux fois dans la liste des exemples de requêtes : une fois pour la règle qui a une action Count et à nouveau pour une règle suivante ou pour l'action par défaut.

Action

Indique si l'action pour la règle correspondante est Allow, Block ou Count.

Heure

Heure à laquelle AWS WAF Classic a reçu la demande d'API Gateway CloudFront ou de votre Application Load Balancer.

4. Pour afficher des informations supplémentaires sur la demande, cliquez sur la flèche située sur le côté gauche de l'adresse IP de cette demande. AWS WAF Classic affiche les informations suivantes :

   IP Source

   La même adresse IP que la valeur dans la colonne Source IP du tableau.

   Pays

   Le code à deux lettres du pays d'où provient la requête. Si le lecteur a utilisé un proxy HTTP ou un Application Load Balancer pour envoyer la demande, il s'agit du code de pays à deux lettres du pays dans lequel se trouve le proxy HTTP ou un Application Load Balancer.

   Pour obtenir une liste des codes de pays à deux lettres et les noms de pays correspondants, consultez la page Wikipédia ISO 3166-1 alpha-2.

   Méthode

   La méthode de requête HTTP pour la requête : `GET`, `HEAD`, `OPTIONS`, `PUT`, `POST`, `PATCH` ou `DELETE`.

   URI

   Le même URI que la valeur de la colonne URI du tableau.

   En-têtes de demandes

   Les en-têtes de requête et les valeurs d'en-tête de la requête.

5. Pour actualiser la liste des exemples de requêtes, choisissez Get new samples.

Utilisation de groupes de règles AWS WAF classiques à utiliser avec AWS Firewall Manager

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Un groupe de règles AWS WAF classique est un ensemble de règles que vous ajoutez à une AWS Firewall Manager politique AWS WAF classique. Vous pouvez créer votre propre groupe de règles ou acheter un groupe de règles géré auprès de AWS Marketplace.

> **Important**
>
> Si vous souhaitez ajouter un groupe de AWS Marketplace règles à votre politique Firewall Manager, chaque compte de votre organisation doit d'abord s'abonner à ce groupe de règles. Une fois que tous les comptes se sont inscrits, vous pouvez ensuite ajouter le groupe de règles à une stratégie. Pour plus d'informations, voir AWS Marketplace groupes de règles.

Rubriques

Création d'un groupe de règles AWS WAF classique

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière

version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
Pour la dernière version de AWS WAF, voirAWS WAF.

Lorsque vous créez un groupe de règles AWS WAF classique à utiliser AWS Firewall Manager, vous spécifiez les règles à ajouter au groupe.

Pour créer un groupe de règles (console)

1. Connectez-vous à l' AWS Management Console aide du compte AWS Firewall Manager administrateur que vous avez configuré dans les conditions requises, puis ouvrez la console Firewall Manager à https://console.aws.amazon.com/wafv2/fms l'adresse.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez Étape 2 : créer un compte administrateur AWS Firewall Manager par défaut.

2. Dans le volet de navigation, choisissez Basculer vers la AWS WAF version classique.
3. Dans le volet de navigation AWS WAF classique, sélectionnez Groupes de règles.
4. Sélectionnez Créer un groupe de règles.

   > **Note**
   >
   > Vous ne pouvez pas ajouter de règles basées sur un débit à un groupe de règles.

5. Si vous avez déjà créé les règles que vous souhaitez ajouter au groupe de règles, choisissez Utiliser les règles existantes pour ce groupe de règles. Si vous souhaitez créer de nouvelles règles à ajouter au groupe de règles, choisissez Créer les règles et les conditions de ce groupe de règles.
6. Choisissez Suivant.
7. Si vous avez choisi de créer des règles, suivez les étapes pour les créer à l'adresse Création d'une règle et ajout de conditions.

> **Note**
>
> Utilisez la console AWS WAF Classic pour créer vos règles.

Lorsque vous avez créé toutes les règles dont vous avez besoin, passez à l'étape suivante.

8. Entrez un nom de groupe de règles.
9. Pour ajouter une règle au groupe de règles, sélectionnez une règle, puis choisissez Add rule (Ajouter une règle). Choisissez si vous souhaitez autoriser, bloquer ou compter les demandes qui correspondent aux conditions de la règle. Pour de plus amples informations sur les options, veuillez consulter Comment fonctionne AWS WAF Classic.
10. Lorsque vous avez fini d'ajouter des règles, choisissez Create (Créer).

Vous pouvez tester votre groupe de règles en l'ajoutant à une AWS WAF WebACL et en définissant l'action WebACL sur Override to Count. Cette action remplace toute action que vous choisissez pour les règles contenues dans le groupe et compte uniquement les demandes correspondantes. Pour plus d'informations, voir Création d'une liste ACL web.

Ajouter et supprimer des règles dans un groupe de règles AWS WAF classique

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Vous pouvez ajouter ou supprimer des règles dans un groupe de règles AWS WAF classique.

La suppression d'une règle du groupe de règles ne permet pas de supprimer la règle elle-même. Elle supprime uniquement la règle du groupe de règles.

Pour ajouter ou supprimer les règles d'un groupe de règles (console)

1. Connectez-vous à l' AWS Management Console aide du compte AWS Firewall Manager administrateur que vous avez configuré dans les conditions requises, puis ouvrez la console Firewall Manager à https://console.aws.amazon.com/wafv2/fms l'adresse.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez Étape 2 : créer un compte administrateur AWS Firewall Manager par défaut.

2. Dans le volet de navigation, choisissez Basculer vers la AWS WAF version classique.
3. Dans le volet de navigation AWS WAF classique, sélectionnez Groupes de règles.
4. Choisissez le groupe de règles que vous souhaitez modifier.
5. Sélectionnez Modifier un groupe de règles.
6. Pour ajouter des règles, effectuez les opérations suivantes :

   a. Sélectionnez une règle, puis choisissez Add rule to rule group (Ajouter une règle au groupe de règles). Choisissez si vous souhaitez autoriser, bloquer ou compter les demandes qui correspondent aux conditions de la règle. Pour de plus amples informations sur les options, veuillez consulter Comment fonctionne AWS WAF Classic. Répétez cette opération pour ajouter d'autres règles au groupe de règles.

      > **Note**
      >
      > Vous ne pouvez pas ajouter de règles basées sur un débit au groupe de règles.

   b. Choisissez Mettre à jour.
7. Pour supprimer des règles, effectuez les opérations suivantes :

   a. Choisissez le signe X en regard de la règle que vous voulez supprimer. Répétez cette opération pour supprimer d'autres règles du groupe de règles.

   b. Choisissez Mettre à jour.

Commencer AWS Firewall Manager à activer les règles AWS WAF classiques

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Vous pouvez l'utiliser AWS Firewall Manager pour activer AWS WAF les règles, les règles AWS WAF classiques, AWS Shield Advanced les protections et les groupes de sécurité Amazon VPC. Les étapes de configuration sont légèrement différentes pour chacun de ces éléments :

- Pour utiliser Firewall Manager afin d'activer les règles à l'aide de la dernière version de AWS WAF, n'utilisez pas cette rubrique. Au lieu de cela, suivez les étapes répertoriées dans Commencer à utiliser les AWS Firewall ManagerAWS WAF politiques.
- Pour utiliser Firewall Manager afin d'activer AWS Shield Advanced les protections, suivez les étapes décrites dansCommencer à utiliser les AWS Firewall ManagerAWS Shield Advanced politiques.
- Pour utiliser Firewall Manager afin d'activer les groupes de sécurité Amazon VPC, suivez les étapes décrites dans. Commencer à utiliser les AWS Firewall Manager politiques des groupes de sécurité Amazon VPC

Pour utiliser Firewall Manager afin d'activer les règles AWS WAF classiques, effectuez les étapes suivantes dans l'ordre.

Rubriques

Étape 1 : Exécuter les prérequis

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez toutes les conditions préalables avant de passer à Étape 2 : Créer des règles.

Étape 2 : Créer des règles

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Au cours de cette étape, vous allez créer des règles à l'aide de la AWS WAF version classique. Si vous avez déjà des règles AWS WAF classiques que vous souhaitez utiliser AWS Firewall Manager, ignorez cette étape et passez àÉtape 3 : Créer un groupe de règles.

> **Note**
>
> Utilisez la console AWS WAF Classic pour créer vos règles.

Pour créer des règles AWS WAF classiques (console)

- Créez vos règles, puis ajoutez vos conditions à vos règles. Pour plus d'informations, consultez Création d'une règle et ajout de conditions.

Vous êtes maintenant prêt à passer à Étape 3 : Créer un groupe de règles.

Étape 3 : Créer un groupe de règles

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Un groupe de règles est un ensemble de règles qui définit les actions à prendre lorsque certaines conditions sont satisfaites. Vous pouvez utiliser des groupes de règles gérés à partir de AWS Marketplace, et vous pouvez créer vos propres groupes de règles. Pour de plus amples informations sur les groupes de règles gérées, reportez-vous à la section AWS Marketplace groupes de règles.

Pour créer votre propre groupe de règles, appliquez la procédure suivante.

Pour créer un groupe de règles (console)

1. Connectez-vous à l' AWS Management Console aide du compte AWS Firewall Manager administrateur que vous avez configuré dans les conditions requises, puis ouvrez la console Firewall Manager à https://console.aws.amazon.com/wafv2/fms l'adresse.
2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Si vous n'avez pas respecté les prérequis, la console affiche les instructions sur la façon de corriger les problèmes. Suivez les instructions, puis recommencez cette étape (créer un groupe de règles). Si vous remplissez les conditions requises, choisissez Fermer.
4. Choisissez Créer une politique.

Pour Type de stratégie, choisissez AWS WAF Classic.

5. Choisissez Créer une AWS Firewall Manager politique et ajoutez un nouveau groupe de règles.
6. Choisissez un Région AWS, puis cliquez sur Suivant.
7. Comme vous avez déjà créé les règles, vous n'avez pas besoin de créer de conditions. Choisissez Suivant.
8. Comme vous avez déjà créé les règles, vous n'avez pas besoin de créer de règles. Choisissez Suivant.
9. Sélectionnez Créer un groupe de règles.
10. Pour Name (Nom), saisissez un nom convivial.
11. Entrez le nom de la CloudWatch métrique que AWS WAF Classic créera et associera au groupe de règles. Le nom ne peut contenir que des caractères alphanumériques (A-Z, a-z, 0-9) ou les caractères spéciaux suivants : _-!"#`+*},./. Il ne peut pas contenir d'espaces.
12. Sélectionnez une règle, puis choisissez Ajouter une règle. Une règle comporte un paramètre d'action qui vous permet de choisir d'autoriser, de bloquer ou de compter les requêtes qui correspondent aux conditions de la règle. Pour ce didacticiel, choisissez Nombre. Répétez l'ajout de règles jusqu'à ce que vous ayez ajouté toutes les règles que vous souhaitiez au groupe de règles.
13. Choisissez Créer.

Vous êtes maintenant prêt à passer à Étape 4 : Création et application d'une politique AWS Firewall ManagerAWS WAF classique.

Étape 4 : Création et application d'une politique AWS Firewall ManagerAWS WAF classique

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Après avoir créé le groupe de règles, vous créez une AWS Firewall Manager AWS WAF politique. Une AWS WAF politique Firewall Manager contient le groupe de règles que vous souhaitez appliquer à vos ressources.

Pour créer une AWS WAF politique Firewall Manager (console)

1. Une fois que vous avez créé le groupe de règles (dernière étape de la procédure précédente, Étape 3 : Créer un groupe de règles), la console affiche la pageRule group summary (Résumé du groupe de règles). Choisissez Suivant.
2. Pour Name (Nom), saisissez un nom convivial.
3. Pour Policy type (Type de stratégie), choisissez WAF.
4. Pour Région, choisissez un Région AWS. Pour protéger les CloudFront ressources d'Amazon, choisissez Global.

   Pour protéger les ressources de plusieurs régions (autres que les CloudFront ressources), vous devez créer des politiques Firewall Manager distinctes pour chaque région.
5. Sélectionnez un groupe de règles à ajouter, puis choisissez Ajouter un groupe de règles.
6. Une stratégie a deux actions possibles : Action définie par un groupe de règles et Nombre. Si vous souhaitez tester la stratégie et le groupe de règles, définissez l'action sur Nombre. Cette action remplace toute action Bloc spécifiée par le groupe de règles contenu dans la stratégie. Autrement dit, si l'action de la stratégie est définie sur Nombre, ces demandes sont uniquement comptabilisées et ne sont pas bloquées. À l'inverse, si vous définissez l'action de la stratégie sur Action définie par un groupe de règles, les actions du groupe de règles de la stratégie sont utilisées. Pour ce didacticiel, choisissez Nombre.
7. Choisissez Suivant.
8. Si vous souhaitez inclure uniquement certains comptes spécifiques dans la stratégie ou exclure des comptes spécifiques de la stratégie, sélectionnez Select accounts to include/exclude from this policy (Sélectionner les comptes à inclure/exclure dans/de cette stratégie) (facultatif). Choisissez Include only these accounts in this policy (Inclure uniquement ces comptes dans cette stratégie) ou Exclude these accounts from this policy (Exclure ces comptes de cette stratégie). Vous ne pouvez choisir qu'une seule option. Choisissez Ajouter. Sélectionnez les numéros de compte à inclure ou à exclure, puis choisissez OK.

> **Note**
>
> Si vous ne sélectionnez pas cette option, Firewall Manager applique une politique à tous les comptes de votre organisation dans AWS Organizations. Si vous ajoutez un nouveau compte à l'organisation, Firewall Manager applique automatiquement la stratégie à ce compte.

9. Choisissez les types de ressource que vous voulez protéger.
10. Si vous souhaitez protéger uniquement les ressources avec des balises spécifiques, ou exclure des ressources avec des balises spécifiques, sélectionnez Utiliser des balises pour inclure/exclure des ressources, entrez les balises et choisissez Inclure ou Exclure. Vous ne pouvez choisir qu'une seule option.

    Si vous entrez plusieurs balises (séparées par des virgules), et si une ressource possède l'une de ces balises, elle est considérée comme une correspondance.

    Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
11. Choisissez Créer et appliquer cette stratégie à des ressources existantes et nouvelles.

    Cette option crée une ACL Web dans chaque compte applicable au sein d'une organisation et associe l'ACL Web aux ressources spécifiées dans les comptes. AWS Organizations Cette option applique également la stratégie à toutes les nouvelles ressources qui correspondent aux précédents critères (type de ressource et balises). Sinon, si vous choisissez Create mais que vous n'appliquez pas cette politique aux ressources existantes ou nouvelles, Firewall Manager crée une ACL Web dans chaque compte applicable au sein de l'organisation, mais n'applique l'ACL Web à aucune ressource. Vous devrez appliquer la stratégie aux ressources ultérieurement.
12. Conservez le paramètre par défaut pour l'option Replace existing associated web ACLs (Remplacer les ACL web associées existantes).

    Lorsque cette option est sélectionnée, Firewall Manager a supprimé toutes les associations d'ACL Web existantes des ressources incluses dans le champ d'application avant de leur associer les ACL Web de la nouvelle politique.
13. Choisissez Suivant.
14. Passez en revue la nouvelle stratégie. Pour effectuer des modifications, sélectionnez Modifier. Lorsque vous êtes satisfait de la politique, choisissez Créer une politique.

Didacticiel : Création d'une stratégie AWS Firewall Manager avec des règles hiérarchiques

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Avec AWS Firewall Manager, vous pouvez créer et appliquer des politiques de protection AWS WAF classiques contenant des règles hiérarchiques. Ainsi, vous pouvez créer et appliquer certaines règles de manière centralisée, mais déléguer à d'autres personnes la création et la maintenance des règles spécifiques à un compte. Vous pouvez surveiller la suppression accidentelle ou mal gérée des règles (communes) appliquées de manière centralisée, ce qui vous garantit que celles-ci sont appliquées de manière cohérente. Les règles spécifiques à un compte ajoutent une protection supplémentaire personnalisée pour les besoins d'équipes individuelles.

> **Note**
>
> Dans la dernière version de AWS WAF, cette fonctionnalité est intégrée et ne nécessite aucune manipulation particulière. Si vous n'utilisez pas encore AWS WAF Classic, utilisez plutôt la dernière version. veuillez consulter Création d'une AWS Firewall Manager politique pour AWS WAF.

Le didacticiel suivant décrit comment créer un ensemble hiérarchique de règles de protection.

Rubriques

Étape 1 : Désigner un compte administrateur de Firewall Manager

Pour l'utiliser AWS Firewall Manager, vous devez désigner un compte de votre organisation en tant que compte administrateur de Firewall Manager. Ce compte peut être le compte de gestion ou un compte de membre de l'organisation.

Vous pouvez utiliser le compte administrateur de Firewall Manager pour créer un ensemble de règles communes que vous pouvez appliquer aux autres comptes de l'organisation. Les autres comptes de l'organisation ne peuvent pas modifier ces règles appliquées de manière centralisée.

Pour désigner un compte en tant que compte administrateur de Firewall Manager et remplir les autres conditions préalables à l'utilisation de Firewall Manager, consultez les instructions figurant dansAWS Firewall Manager prérequis. Si vous avez déjà réuni les conditions requises, vous pouvez passer directement à l'étape 2 de ce didacticiel.

Dans ce didacticiel, nous faisons référence au compte administrateur sous la dénomination **`Firewall-Administrator-Account`**.

Étape 2 : créer un groupe de règles à l'aide du compte administrateur de Firewall Manager

Ensuite, créez un groupe de règles à l'aide de **`Firewall-Administrator-Account`**. Ce groupe de règles contient les règles communes que vous appliquerez à tous les comptes membres régis par la stratégie que vous allez créer dans l'étape suivante. Seul le compte **`Firewall-Administrator-Account`** peut apporter des modifications à ces règles et au groupe de règles de conteneur.

Dans ce didacticiel, nous faisons référence à ce groupe de règles de conteneur sous la dénomination **`Common-Rule-Group`**.

Pour créer un groupe de règles, suivez les instructions dans Création d'un groupe de règles AWS WAF classique. N'oubliez pas de vous connecter à la console à l'aide de votre compte administrateur Firewall Manager (**`Firewall-Administrator-Account`**) lorsque vous suivez ces instructions.

Étape 3 : créer une politique Firewall Manager et associer le groupe de règles communes

À l'aide de**Firewall-Administrator-Account**, créez une politique Firewall Manager. Lorsque vous créez cette stratégie, vous devez procéder comme suit :

- Ajoutez **Common-Rule-Group** à la nouvelle stratégie.
- Incluez tous les comptes de l'organisation auxquels vous souhaitez appliquer **Common-Rule-Group**.
- Ajoutez toutes les ressources auxquelles vous souhaitez appliquer **Common-Rule-Group**.

Pour obtenir des instructions sur la création d'une stratégie, consultez Création d'une AWS Firewall Manager politique.

Cela crée une liste ACL web dans chaque compte spécifié et ajoute **Common-Rule-Group** à chacune de ces listes ACL web. Une fois que vous avez créé la stratégie, cette liste ACL web et les règles communes sont déployées pour tous les comptes spécifiés.

Dans ce didacticiel, nous faisons référence à cette liste ACL web sous la dénomination **Administrator-Created-ACL**. Une liste **Administrator-Created-ACL** unique existe désormais dans chaque compte membre spécifié de l'organisation.

Étape 4 : Ajouter des règles spécifiques à un compte

Chaque compte membre de l'organisation peut maintenant ajouter ses propres règles spécifiques à la liste **Administrator-Created-ACL** qui figure dans son compte. Les règles communes déjà en vigueur **Administrator-Created-ACL** continuent de s'appliquer, de même que les nouvelles règles spécifiques aux comptes. AWS WAF inspecte les requêtes Web en fonction de l'ordre dans lequel les règles apparaissent dans l'ACL Web. Cela s'applique à la fois à la liste **Administrator-Created-ACL** et aux règles spécifiques à un compte.

Pour ajouter des règles à**Administrator-Created-ACL**, voirModification d'une ACL Web.

Conclusion

Vous disposez désormais d'une ACL Web qui contient des règles communes administrées par le compte administrateur de Firewall Manager ainsi que des règles spécifiques au compte gérées par chaque compte membre.

La liste **`Administrator-Created-ACL`** dans chaque compte fait référence au groupe unique **`Common-Rule-Group`**. Par conséquent, les futures modifications apportées par le compte administrateur de **`Common-Rule-Group`** Firewall Manager prendront effet immédiatement dans chaque compte membre.

Les comptes membres ne peuvent pas modifier ou supprimer les règles communes dans **`Common-Rule-Group`**.

Les règles spécifiques à un compte n'affectent pas les autres comptes.

Journalisation des informations de trafic de la liste ACL web

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

> **Note**
>
> Vous ne pouvez pas utiliser Amazon Security Lake pour collecter des données AWS WAF classiques.

Vous pouvez activer la journalisation pour obtenir des informations détaillées sur le trafic qui est analysé par votre liste ACL web. Les informations contenues dans les journaux incluent l'heure à laquelle AWS WAF Classic a reçu la demande de votre AWS ressource, des informations détaillées sur la demande et l'action pour la règle à laquelle chaque demande correspondait.

Pour commencer, vous devez configurer un Amazon Kinesis Data Firehose. Dans le cadre de ce processus, vous choisissez une destination pour stocker vos journaux. Ensuite, vous choisissez la liste ACL web pour laquelle vous souhaitez activer la journalisation. Une fois que vous avez activé la journalisation, elle AWS WAF envoie les journaux via le Firehose à votre destination de stockage.

Pour plus d'informations sur la façon de créer un Amazon Kinesis Data Firehose et de consulter vos journaux enregistrés, consultez What Is Amazon Data Firehose ? Pour comprendre les autorisations requises pour votre configuration Kinesis Data Firehose, consultez la section Contrôle des accès avec Amazon Kinesis Data Firehose.

Vous devez disposer des autorisations suivantes pour activer la journalisation :

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `waf:PutLoggingConfiguration`

Pour de plus amples informations sur les rôles liés au service et l'autorisation `iam:CreateServiceLinkedRole`, veuillez consulter Utilisation de rôles liés à un service pour Classic AWS WAF.

Pour activer la journalisation pour une liste ACL web

1. Créez un Amazon Kinesis Data Firehose en utilisant un nom commençant par le aws-waf-logs préfixe « - » Par exemple,. `aws-waf-logs-us-east-2-analytics` Créez le firehose de données avec une source PUT et dans la région où vous développez vos activités. Si vous capturez des journaux pour Amazon CloudFront, créez le firehose dans l'est des États-Unis (Virginie du Nord). Pour plus d'informations, consultez Création d'un flux de diffusion Amazon Data Firehose.

   > **Important**
   >
   > Ne choisissez pas `Kinesis stream` en tant que source.
   > Un journal AWS WAF classique équivaut à un enregistrement Firehose. Si vous recevez généralement 10 000 requêtes par seconde et que vous activez les journaux complets, vous devriez avoir un paramètre de 10 000 enregistrements par seconde dans Firehose. Si vous ne configurez pas Firehose correctement, AWS WAF Classic n'enregistrera pas tous les journaux. Pour de plus amples informations, veuillez consulter Amazon Kinesis Data Firehose Quotas (Quotas d'Amazon Kinesis Data Firehose).

2. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

Si le bouton Passer à la AWS WAF version classique apparaît dans le volet de navigation, sélectionnez-le.

3. Dans le volet de navigation, choisissez Web ACLs.
4. Choisissez le nom de l'ACL Web pour laquelle vous souhaitez activer la journalisation. Cela ouvre une page contenant les détails de l'ACL Web dans le volet droit.
5. Dans l'onglet Journalisation, choisissez Activer la journalisation.
6. Choose the Kinesis Data Firehose que vous avez créé à la première étape. Vous devez choisir une lance à incendie qui commence par « aws-waf-logs - ».
7. (Facultatif) Si vous ne souhaitez pas que certains champs et leurs valeurs soient inclus dans les journaux, censurez ces champs. Choisissez le champ à censurer, puis choisissez Ajouter. Répétez si nécessaire pour censurer des champs supplémentaires. Les champs censurés apparaîtront en tant que `REDACTED` dans les journaux. Par exemple, si vous censurez le champ cookie, le champ cookie dans les journaux apparaîtra comme `REDACTED`.
8. Choisissez Activer la journalisation.

> **Note**
>
> Lorsque vous activez correctement la journalisation, AWS WAF Classic crée un rôle lié à un service doté des autorisations nécessaires pour écrire des journaux sur Amazon Kinesis Data Firehose. Pour plus d'informations, consultez Utilisation de rôles liés à un service pour Classic AWS WAF.

Pour désactiver la journalisation pour une liste ACL web

1. Dans le volet de navigation, choisissez Web ACLs.
2. Choisissez le nom de l'ACL Web pour laquelle vous souhaitez désactiver la journalisation. Cela ouvre une page contenant les détails de l'ACL Web dans le volet droit.
3. Dans l'onglet Journalisation, choisissez Désactiver la journalisation.
4. Dans la boîte de dialogue, sélectionnez Désactiver la journalisation.

Example Exemple de journal

```
{
```

```
"timestamp":1533689070589,
"formatVersion":1,
"webaclId":"385cb038-3a6f-4f2f-ac64-09ab912af590",
"terminatingRuleId":"Default_Action",
"terminatingRuleType":"REGULAR",
"action":"ALLOW",
"httpSourceName":"CF",
"httpSourceId":"i-123",
"ruleGroupList":[
                        {
                         "ruleGroupId":"41f4eb08-4e1b-2985-92b5-e8abf434fad3",
                         "terminatingRule":null,
                         "nonTerminatingMatchingRules":[
                                                         {"action" : "COUNT",
                                                         "ruleId" :
"4659b169-2083-4a91-bbd4-08851a9aaf74"}
                                                        ],
                         "excludedRules":               [
                                                         {"exclusionType" :
"EXCLUDED_AS_COUNT",
                                                          "ruleId" :
"5432a230-0113-5b83-bbb2-89375c5bfa98"}
                                                        ]
                        }
                       ],

"rateBasedRuleList":[
                            {
                             "rateBasedRuleId":"7c968ef6-32ec-4fee-96cc-51198e412e7f",

                             "limitKey":"IP",
                             "maxRateAllowed":100

                            },
                            {
                             "rateBasedRuleId":"462b169-2083-4a93-bbd4-08851a9aaf30",
                             "limitKey":"IP",
                             "maxRateAllowed":100
                             }
                             ],

"nonTerminatingMatchingRules":[
```

```
                                        {"action" : "COUNT",

                                        "ruleId" : "4659b181-2011-4a91-
bbd4-08851a9aaf52"}
                                       ],

 "httpRequest":{
                      "clientIp":"192.10.23.23",

                      "country":"US",

                      "headers":[

                                  {
                                   "name":"Host",
                                   "value":"127.0.0.1:1989"
                                  },
                                  {
                                   "name":"User-Agent",
                                   "value":"curl/7.51.2"
                                  },
                                  {
                                   "name":"Accept",
                                   "value":"*/*"
                                  }
                                 ],
                     "uri":"REDACTED",
                     "args":"usernam=abc",
                     "httpVersion":"HTTP/1.1",
                     "httpMethod":"GET",
                     "requestId":"cloud front Request id"
                     }
}
```

Voici une explication de chaque élément répertorié dans ces journaux :

timestamp

L'horodatage en millisecondes.

formatVersion

Version du format du journal.

webaclId

GUID de la liste ACL Web.

terminatingRuleId

ID de la règle qui a résilié la requête. Si rien ne résilie la requête, la valeur est `Default_Action`.

terminatingRuleType

Type de règle qui a résilié la requête. Valeurs possibles : RATE_BASED, REGULAR et GROUP.

action

L'action. Valeurs possibles pour une règle de résiliation : ALLOW et BLOCK. COUNT n'est pas une valeur valide pour une règle de résiliation.

terminatingRuleMatchDétails

Informations détaillées sur la règle de fin correspondant à la demande. Une règle de fin comporte une action qui met fin au processus d'inspection par rapport à une demande Web. Les actions possibles pour une règle de terminaison sont ALLOW et BLOCK. Cette information n'est renseignée que pour les instructions de règle de correspondance d'injection SQL et de script inter-site (XSS). Comme pour toutes les instructions de règle qui inspectent plusieurs éléments, AWS WAF applique l'action sur la première correspondance et arrête l'inspection de la demande Web. Une demande Web avec une action de fin peut contenir d'autres menaces, en plus de celle signalée dans le journal.

httpSourceName

Source de la requête. Valeurs possibles : CF (si la source est Amazon CloudFront), APIGW (si la source est Amazon API Gateway) et ALB (si la source est un Application Load Balancer).

httpSourceId

ID de la source. Ce champ indique l'ID de la CloudFront distribution Amazon associée, l'API REST pour API Gateway ou le nom d'un Application Load Balancer.

ruleGroupList

Liste des groupes de règles qui ont agi sur cette requête. Dans l'exemple de code précédent, il n'y en a qu'un seul.

ruleGroupId

ID du groupe de règles. Si la règle a bloqué la requête, l'ID pour `ruleGroupID` est le même que pour `terminatingRuleId`.

terminatingRule

Règle au sein du groupe de règles qui a résilié la requête. Si la valeur est non nulle, elle contient également un ruleid et une action. Dans ce cas, l'action est toujours BLOCK.

nonTerminatingMatchingRègles

Liste des règles dans le groupe de règles qui correspondent à la requête. Il s'agit toujours de règles COUNT (règles de non-résiliation correspondantes).

action (groupe de nonTerminatingMatching règles)

Il s'agit toujours de COUNT (règles de non-résiliation correspondantes).

RuleID nonTerminatingMatching (groupe de règles)

ID de la règle au sein du groupe de règles qui correspond à la requête et n'était pas de résiliation. Autrement dit, des règles COUNT.

excludedRules

Liste des règles dans le groupe de règles que vous avez exclues. L'action pour ces règles est définie sur COUNT.

exclusionType (groupe excludedRules)

Type qui indique que la règle exclue comporte l'action COUNT.

ruleId (groupe excludedRules)

ID de la règle au sein du groupe de règles qui est exclu.

rateBasedRuleListe

Liste de règles basées sur le débit qui ont agi sur la requête.

rateBasedRuleId

ID de la règle basée sur le débit qui a agi sur la requête. Si cette règle a résilié la requête, l'ID pour `rateBasedRuleId` est le même que pour `terminatingRuleId`.

limitKey

Champ AWS WAF utilisé pour déterminer si les demandes sont susceptibles de provenir d'une source unique et sont donc soumises à un suivi du taux. Valeur possible : IP.

maxRateAllowed

Nombre maximal de requêtes, qui ont une valeur identique dans le champ spécifié par `limitKey`, autorisées au cours d'une période de cinq minutes. Si le nombre de demandes dépasse le nombre de prédicats spécifiés dans la règle `maxRateAllowed` et si les autres prédicats spécifiés dans la règle sont également satisfaits, AWS WAF déclenche l'action spécifiée pour cette règle.

httpRequest

Métadonnées relatives à la requête.

clientIp

Adresse IP du client envoyant la requête.

country

Pays source de la requête. S'il n' AWS WAF est pas en mesure de déterminer le pays d'origine, il définit ce champ sur `-`.

headers

Liste des en-têtes.

uri

URI de la requête. L'exemple de code précédent montre ce que la valeur serait si ce champ avait été censuré.

args

Chaîne de requête.

httpVersion

Version de HTTP.

httpMethod

Méthode HTTP de la requête.

requestId

ID de la demande.

Affichage des adresses IP bloquées par une règle basée sur un débit

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

AWS WAF Classic fournit une liste d'adresses IP bloquées par des règles basées sur le taux.

Pour afficher les adresses bloquées par une règle basée sur un débit

1. Connectez-vous à la AWS WAF console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

   Si vous voyez Passer à la AWS WAF version classique dans le volet de navigation, sélectionnez-le.
2. Dans le volet de navigation, choisissez Règles.
3. Dans la colonne Name, choisissez une règle basée sur un débit.

   La liste affiche les adresses IP que la règle bloque actuellement.

Comment AWS WAF Classic fonctionne avec les CloudFront fonctionnalités d'Amazon

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière

version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
Pour la dernière version de AWS WAF, voirAWS WAF.

Lorsque vous créez une ACL Web, vous pouvez spécifier une ou plusieurs CloudFront distributions que AWS WAF Classic doit inspecter. AWS WAF Classic commence à autoriser, à bloquer ou à compter les requêtes Web pour ces distributions en fonction des conditions que vous identifiez dans l'ACL Web. CloudFront fournit certaines fonctionnalités qui améliorent les fonctionnalités AWS WAF classiques. Ce chapitre décrit quelques méthodes que vous pouvez configurer CloudFront pour que AWS WAF Classic CloudFront et Classic fonctionnent mieux ensemble.

Rubriques

Utilisation de AWS WAF Classic avec des pages d'erreur CloudFront personnalisées

Lorsque AWS WAF Classic bloque une requête Web en fonction des conditions que vous spécifiez, il renvoie le code d'état HTTP 403 (Interdit) à CloudFront. CloudFront Renvoie ensuite ce code d'état au visualiseur. La visionneuse affiche ensuite un court message par défaut peu formaté similaire au message suivant :

```
Forbidden: You don't have permission to access /myfilename.html on this server.
```

Si vous préférez afficher un message d'erreur personnalisé, éventuellement en utilisant le même format que le reste de votre site Web, vous pouvez configurer CloudFront pour renvoyer au lecteur un objet (par exemple, un fichier HTML) contenant votre message d'erreur personnalisé.

> **Note**
>
> CloudFront Impossible de faire la distinction entre un code d'état HTTP 403 renvoyé par votre origine et un code renvoyé par AWS WAF Classic lorsqu'une requête est bloquée. Par

conséquent, vous ne pouvez pas renvoyer différentes pages d'erreur personnalisées en fonction des différentes causes d'un code de statut HTTP 403.

Pour plus d'informations sur les pages d'erreur CloudFront personnalisées, consultez la section Personnalisation des réponses aux erreurs dans le manuel Amazon CloudFront Developer Guide.

Utilisation de AWS WAF Classic CloudFront pour les applications exécutées sur votre propre serveur HTTP

Lorsque vous utilisez AWS WAF Classic avec CloudFront, vous pouvez protéger vos applications exécutées sur n'importe quel serveur Web HTTP, qu'il s'agisse d'un serveur Web exécuté dans Amazon Elastic Compute Cloud (Amazon EC2) ou d'un serveur Web que vous gérez en privé. Vous pouvez également configurer CloudFront pour exiger le protocole HTTPS entre CloudFront et votre propre serveur Web, ainsi qu'entre les utilisateurs et CloudFront.

Exiger le protocole HTTPS entre votre propre serveur Web CloudFront et votre propre serveur Web

Pour exiger le protocole HTTPS entre votre propre serveur Web CloudFront et votre propre serveur Web, vous pouvez utiliser la fonctionnalité d'origine CloudFront personnalisée et configurer la politique du protocole d'origine et les paramètres du nom de domaine d'origine pour des origines spécifiques. Dans votre CloudFront configuration, vous pouvez spécifier le nom DNS du serveur ainsi que le port et le protocole que vous souhaitez utiliser CloudFront pour récupérer des objets depuis votre origine. Vous devez également vous assurer que le certificat SSL/TLS sur votre serveur d'origine personnalisé correspond au nom de domaine d'origine que vous avez configuré. Lorsque vous utilisez votre propre serveur Web HTTP en dehors de AWS, vous devez utiliser un certificat signé par une autorité de certification (CA) tierce de confiance, par exemple Comodo ou DigiCert Symantec. Pour plus d'informations sur l'exigence du protocole HTTPS pour les communications entre votre propre serveur Web CloudFront et votre propre serveur Web, consultez la rubrique Exiger le protocole HTTPS pour la communication entre CloudFront et votre origine personnalisée dans le manuel Amazon CloudFront Developer Guide.

Exiger le protocole HTTPS entre un utilisateur et CloudFront

Pour exiger le protocole HTTPS entre les spectateurs et CloudFront, vous pouvez modifier la politique du protocole de visionnage pour un ou plusieurs comportements de cache dans votre CloudFront distribution. Pour plus d'informations sur l'utilisation du protocole HTTPS entre utilisateurs CloudFront, consultez la rubrique Requirement du protocole HTTPS pour la communication entre

utilisateurs et CloudFront dans le manuel Amazon CloudFront Developer Guide. Vous pouvez également apporter votre propre certificat SSL afin que les utilisateurs puissent se connecter à votre CloudFront distribution via HTTPS en utilisant votre propre nom de domaine, par exemple https://www.mysite.com. Pour plus d'informations, consultez la rubrique Configuration des noms de domaine alternatifs et du protocole HTTPS dans le manuel Amazon CloudFront Developer Guide.

Choix des méthodes HTTP qui CloudFront répondent à

Lorsque vous créez une distribution CloudFront Web Amazon, vous choisissez les méthodes HTTP que vous CloudFront souhaitez traiter et transmettre à votre source. Choisissez parmi les options suivantes :

- GET, HEAD — Vous ne pouvez l'utiliser CloudFront que pour récupérer des objets depuis votre origine ou pour obtenir des en-têtes d'objets.
- GET, HEAD, OPTIONS — Vous CloudFront ne pouvez les utiliser que pour obtenir des objets depuis votre origine, obtenir des en-têtes d'objets ou récupérer une liste des options prises en charge par votre serveur d'origine.
- GET, HEAD, OPTIONS, PUT, POST, PATCH, DELETE — Vous pouvez les utiliser CloudFront pour obtenir, ajouter, mettre à jour et supprimer des objets, ainsi que pour obtenir des en-têtes d'objets. De plus, vous pouvez exécuter d’autres opérations POST telles que l’envoi de données à partir d’un formulaire web.

Vous pouvez également utiliser les conditions AWS WAF classiques de correspondance de chaînes pour autoriser ou bloquer les demandes en fonction de la méthode HTTP, comme décrit dansUtilisation des conditions de correspondance de chaîne. Si vous souhaitez utiliser une combinaison de méthodes compatibles CloudFront , telles que `GET` et`HEAD`, vous n'avez pas besoin de configurer AWS WAF Classic pour bloquer les demandes utilisant les autres méthodes. Si vous souhaitez autoriser une combinaison de méthodes non CloudFront compatibles, telles que, et `GET` `HEAD``POST`, vous pouvez configurer CloudFront pour répondre à toutes les méthodes, puis utiliser AWS WAF Classic pour bloquer les demandes utilisant d'autres méthodes.

Pour plus d'informations sur le choix des méthodes qui CloudFront répondent, consultez la section Méthodes HTTP autorisées dans la rubrique Valeurs que vous spécifiez lors de la création ou de la mise à jour d'une distribution Web du manuel Amazon CloudFront Developer Guide.

Sécurité dans AWS WAF Classic

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. L'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS WAF Classic, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation ainsi que les lois et réglementations applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de AWS WAF Classic. Les rubriques suivantes expliquent comment configurer AWS WAF Classic pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources AWS WAF Classic.

Rubriques

- Gestion des identités et des accès pour AWS WAF Classic
- Journalisation et surveillance dans la AWS WAF version classique
- Validation de conformité pour AWS WAF Classic
- Résilience dans AWS WAF Classic
- Sécurité de l'infrastructure dans AWS WAF Classic

Protection des données dans AWS WAF Classic

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS WAF Classic. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.

- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec AWS WAF Classic ou autre à Services AWS l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

AWS WAF Les entités classiques, telles que les ACL, les règles et les conditions Web, sont chiffrées au repos, sauf dans certaines régions où le chiffrement n'est pas disponible, notamment en Chine (Pékin) et en Chine (Ningxia). Des clés de chiffrement uniques sont utilisées pour chaque région.

Supprimer des ressources AWS WAF classiques

Vous pouvez supprimer les ressources que vous créez dans AWS WAF Classic. Consultez les instructions relatives à chaque type de ressource dans les sections suivantes.

- Suppression d'une liste ACL web
- Ajouter et supprimer des règles dans un groupe de règles AWS WAF classique
- Suppression d'une règle

Gestion des identités et des accès pour AWS WAF Classic

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources AWS WAF Classic. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans AWS WAF Classic.

Utilisateur du service : si vous utilisez le service AWS WAF Classic pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités AWS WAF classiques pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires.

En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans la AWS WAF version classique, consultezRésolution des problèmes d'identité et d'accès AWS WAF classiques.

Administrateur du service — Si vous êtes responsable des ressources AWS WAF Classic au sein de votre entreprise, vous avez probablement un accès complet à AWS WAF Classic. Il vous incombe de déterminer à quelles fonctionnalités et ressources AWS WAF Classic les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec AWS WAF Classic, consultezComment AWS WAF Classic fonctionne avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à AWS WAF Classic. Pour consulter des exemples de politiques AWS WAF classiques basées sur l'identité que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour Classic AWS WAF

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide

de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède en utilisant les informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour

obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour

obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés

à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui

autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux

politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS WAF Classic fonctionne avec IAM

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Avant d'utiliser IAM pour gérer l'accès à AWS WAF Classic, découvrez quelles fonctionnalités IAM sont disponibles avec AWS WAF Classic.

Fonctionnalités IAM que vous pouvez utiliser avec Classic AWS WAF

Fonction IAM	AWS WAF Support classique
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACL	Non

Fonction IAM	AWS WAF Support classique
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Fonctions de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont AWS WAF Classic et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Classic AWS WAF

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Pour consulter des exemples de politiques AWS WAF classiques basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Classic AWS WAF

Politiques basées sur les ressources dans Classic AWS WAF

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour AWS WAF Classic

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom

que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions AWS WAF classiques, voir Actions définies par AWS WAF et Actions définies par AWS WAF Regional dans la référence d'autorisation de service.

Dans AWS WAF Classic, les actions de stratégie utilisent le préfixe suivant avant l'action :

```
waf
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "waf:action1",
      "waf:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions commençant par « AWS WAF Classic »`List`, incluez l'action suivante :

```
"Action": "waf:List*"
```

Pour consulter des exemples de politiques AWS WAF classiques basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Classic AWS WAF

Ressources relatives aux politiques pour AWS WAF Classic

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources AWS WAF classiques et de leurs ARN, voir Ressources définies par AWS WAF et Ressources définies par AWS WAF Regional dans la référence d'autorisation de service. Pour savoir avec quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez les sections Actions définies par AWS WAF et Actions définies par AWS WAF Regional. Pour autoriser ou refuser l'accès à un sous-ensemble de ressources AWS WAF classiques, incluez l'ARN de la ressource dans l'`resource`élément de votre politique.

Dans AWS WAF Classic, les ressources sont des ACL et des règles Web. AWS WAF Classic prend également en charge des conditions telles que la correspondance d'octets, la correspondance IP et la contrainte de taille.

Ces ressources et conditions ont des noms ARN (Amazon Resource Name) uniques associés, comme cela est illustré dans le tableau suivant.

Nom dans la AWS WAF console	Nom dans le AWS WAF SDK/CLI	Format ARN
Liste ACL web	`WebACL`	`arn:aws:waf:: account:webacl/ID`
Règle	`Rule`	`arn:aws:waf:: account:rule/ID`
Condition de correspondance de chaîne	`ByteMatchSet`	`arn:aws:waf:: account:bytematchset /ID`

Nom dans la AWS WAF console	Nom dans le AWS WAF SDK/CLI	Format ARN	
Condition de correspondance d'injection SQL	`SqlInjectionMatchSet`	`arn:aws:waf::` *`account`*`:`*`sqlinjectionset`* `/`*`ID`*	
Condition de contrainte de taille	`SizeConstraintSet`	`arn:aws:waf::` *`account`*`:`*`sizeconstraintset`* `/`*`ID`*	
Condition de correspondance IP	`IPSet`	`arn:aws:waf::` *`account`*`:`*`ipset`*`/`*`ID`*	
Condition de correspondance de scripts inter-site	`XssMatchSet`	`arn:aws:waf::` *`account`*`:`*`xssmatchset`* `/`*`ID`*	

Pour autoriser ou refuser l'accès à un sous-ensemble de ressources AWS WAF classiques, incluez l'ARN de la ressource dans l'`resource`élément de votre politique. Les ARN pour AWS WAF Classic ont le format suivant :

```
arn:aws:waf::account:resource/ID
```

Remplacez les variables *`compte`*, *`ressources`* et *`ID`* variables par des valeurs valides. Les valeurs valides peuvent être les suivantes :

- *`compte`* : L'identifiant de votre Compte AWS. Vous devez spécifier une valeur.
- *`ressource`* : type de ressource AWS WAF classique.
- *`ID`* : ID de la ressource AWS WAF classique, ou un caractère générique (*) pour indiquer toutes les ressources du type spécifié associées à la ressource spécifiée Compte AWS.

Par exemple, l'ARN suivante spécifie toutes les listes ACL web pour le compte 111122223333 :

```
arn:aws:waf::111122223333:webacl/*
```

Clés de conditions de politique pour AWS WAF Classic

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition AWS WAF classiques, voir Clés de condition AWS WAF et ressources définies par AWS WAF Regional dans la référence d'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez les sections Actions définies par AWS WAF et Actions définies par AWS WAF Regional.

Pour consulter des exemples de politiques AWS WAF classiques basées sur l'identité, consultez. Exemples de politiques basées sur l'identité pour Classic AWS WAF

ACL en version classique AWS WAF

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Classic AWS WAF

Prise en charge d'ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les

étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec AWS WAF Classic

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Sessions d'accès transféré pour AWS WAF Classic

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux

services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour AWS WAF Classic

Prend en charge les fonctions du service	Oui

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités AWS WAF classiques. Modifiez les rôles de service uniquement lorsque AWS WAF Classic fournit des instructions à cet effet.

Rôles liés à un service pour Classic AWS WAF

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus de détails sur la création ou la gestion des rôles liés à un service AWS WAF classique, consultez. Utilisation de rôles liés à un service pour Classic AWS WAF

Exemples de politiques basées sur l'identité pour Classic AWS WAF

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources AWS WAF classiques. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d’effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM doit créer des politiques IAM. L’administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l’identité IAM à l’aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l’onglet JSON dans le Guide de l’utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par AWS WAF Classic, y compris le format des ARN pour chacun des types de ressources, voir Actions, ressources et clés de condition pour AWS WAF et Actions, ressources et clés de condition pour AWS WAF Regional dans la référence d'autorisation de service.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console AWS WAF Classic
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources AWS WAF classiques dans votre compte. Ces actions peuvent entraîner des frais pour

votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez Politiques gérées AWS ou Politiques gérées AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège - Lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès - Vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles - IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console AWS WAF Classic

Pour accéder à la console AWS WAF Classic, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les détails des ressources AWS WAF classiques de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Les utilisateurs autorisés à accéder à la AWS console et à l'utiliser peuvent également accéder à la console AWS WAF classique. Aucune autorisation supplémentaire n'est requise.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
```

```
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Résolution des problèmes d'identité et d'accès AWS WAF classiques

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS WAF Classic et IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS WAF Classic
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources AWS WAF classiques

Je ne suis pas autorisé à effectuer une action dans AWS WAF Classic

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `waf:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 waf:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `waf:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transférer un rôle à AWS WAF Classic.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans AWS WAF Classic. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les stratégies de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources AWS WAF classiques

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si AWS WAF Classic prend en charge ces fonctionnalités, consultezComment AWS WAF Classic fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Utilisation de rôles liés à un service pour Classic AWS WAF

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

AWS WAF Utilise les rôles AWS Identity and Access Management liés au service (IAM) de façon classique. Un rôle lié à un service est un type unique de rôle IAM directement lié à Classic. AWS WAF Les rôles liés à un service sont prédéfinis par AWS WAF Classic et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration de AWS WAF Classic, car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. AWS WAF Classic définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS WAF Classic peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisations. Cette politique d'autorisations ne peut pas être attachée à une autre entité IAM.

Vous ne pouvez supprimer un rôle lié à un service qu’après avoir supprimé les ressources connexes du rôle. Cela protège vos ressources AWS WAF Classic, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour Classic AWS WAF

AWS WAF Classic utilise les rôles liés aux services suivants :

- `AWSServiceRoleForWAFLogging`
- `AWSServiceRoleForWAFRegionalLogging`

AWS WAF Classic utilise ces rôles liés à des services pour écrire des journaux sur Amazon Data Firehose. Ces rôles ne sont utilisés que si vous activez la connexion AWS WAF. Pour plus d’informations, consultez Journalisation des informations de trafic de la liste ACL web.

Les rôles `AWSServiceRoleForWAFLogging` et `AWSServiceRoleForWAFRegionalLogging` liés à un service font confiance aux services suivants (respectivement) pour assumer le rôle :

- `waf.amazonaws.com`

  `waf-regional.amazonaws.com`

Les politiques d'autorisation des rôles permettent à AWS WAF Classic d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `firehose:PutRecord` et `firehose:PutRecordBatch` sur les ressources de flux de données Amazon Data Firehose dont le nom commence par « aws-waf-logs - ». Par exemple, `aws-waf-logs-us-east-2-analytics`.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Création d'un rôle lié à un service pour Classic AWS WAF

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez la connexion AWS WAF classique sur le AWS Management Console, ou que vous faites une `PutLoggingConfiguration` demande dans la CLI AWS WAF classique ou l'API AWS WAF classique, AWS WAF Classic crée le rôle lié au service pour vous.

Vous devez disposez de l'autorisation `iam:CreateServiceLinkedRole` pour activer la journalisation.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous activez la journalisation AWS WAF classique, AWS WAF Classic crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour Classic AWS WAF

AWS WAF Classic ne vous permet pas de modifier les rôles `AWSServiceRoleForWAFLogging` et les rôles `AWSServiceRoleForWAFRegionalLogging` liés à un service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l’aide d’IAM. Pour plus d’informations, consultez Modification d’un rôle lié à un service dans le Guide de l’utilisateur IAM.

Supprimer un rôle lié à un service pour Classic AWS WAF

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n’avez aucune entité inutilisée

qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service AWS WAF Classic utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources AWS WAF classiques utilisées par **`AWSServiceRoleForWAFLogging`** et **`AWSServiceRoleForWAFRegionalLogging`**

1. Sur la console AWS WAF Classic, supprimez la journalisation de chaque ACL Web. Pour plus d'informations, consultez Journalisation des informations de trafic de la liste ACL web.
2. Au moyen de l'API ou de l'interface de ligne de commande, envoyez une requête `DeleteLoggingConfiguration` pour chaque liste ACL web avec la journalisation activée. Pour plus d'informations, consultez la section AWS WAF Classic API Reference.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, la CLI IAM ou l'API IAM pour supprimer les rôles liés à un service`AWSServiceRoleForWAFLogging`. `AWSServiceRoleForWAFRegionalLogging` Pour plus d'informations, veuillez consulter Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les AWS WAF rôles classiques liés à un service

AWS WAF Classic prend en charge l'utilisation de rôles liés à un service dans les sections suivantes. Régions AWS

Nom de la région	Identité de la région	Support dans la AWS WAF version classique
USA Est (Virginie du Nord)	`us-east-1`	Oui
USA Est (Ohio)	`us-east-2`	Oui
USA Ouest (Californie du Nord)	`us-west-1`	Oui

Nom de la région	Identité de la région	Support dans la AWS WAF version classique
USA Ouest (Oregon)	us-west-2	Oui
Asie-Pacifique (Mumbai)	ap-south-1	Oui
Asie-Pacifique (Osaka)	ap-northeast-3	Oui
Asie-Pacifique (Séoul)	ap-northeast-2	Oui
Asie-Pacifique (Singapour)	ap-southeast-1	Oui
Asie-Pacifique (Sydney)	ap-southeast-2	Oui
Asie-Pacifique (Tokyo)	ap-northeast-1	Oui
Canada (Centre)	ca-central-1	Oui
Europe (Francfort)	eu-central-1	Oui
Europe (Irlande)	eu-west-1	Oui
Europe (Londres)	eu-west-2	Oui
Europe (Paris)	eu-west-3	Oui
Amérique du Sud (São Paulo)	sa-east-1	Oui

Journalisation et surveillance dans la AWS WAF version classique

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de AWS WAF Classic et de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. AWS fournit plusieurs outils pour surveiller vos ressources AWS WAF Classic et répondre à des événements potentiels :

CloudWatch Alarmes Amazon

À l'aide d' CloudWatch alarmes, vous observez une seule métrique sur une période que vous spécifiez. Si la métrique dépasse un seuil donné, CloudWatch envoie une notification à une rubrique ou AWS Auto Scaling à une politique Amazon SNS. Pour plus d’informations, consultez Surveillance avec Amazon CloudWatch.

AWS CloudTrail Journaux

CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS WAF Classic. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à AWS WAF Classic, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires. Pour plus d'informations, voir Journalisation des appels d'API AWS CloudTrail avec.

Validation de conformité pour AWS WAF Classic

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

  > **Note**
  >
  > Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.

- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS WAF Classic

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l'infrastructure dans AWS WAF Classic

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

En tant que service géré, AWS WAF Classic est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure

est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à AWS WAF Classic via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

AWS WAF Quotas classiques

> **Note**
>
> Il s'agit d'une documentation AWS WAF classique. Vous ne devez utiliser cette version que si vous avez créé AWS WAF des ressources, telles que des règles et des ACL Web, AWS WAF avant novembre 2019, et que vous ne les avez pas encore migrées vers la dernière version. Pour migrer vos ressources, veuillez consulter Migration de vos ressources AWS WAF classiques vers AWS WAF.
> Pour la dernière version de AWS WAF, voirAWS WAF.

AWS WAF Classic est soumis aux quotas suivants (anciennement appelés limites).

AWS WAF Classic dispose de quotas par défaut sur le nombre d'entités par compte et par région. Vous pouvez demander leur augmentation.

Ressource	Quota par défaut par compte et par région
Liste ACL web	50
Règles	100
R ate-based-rules	5
Conditions par compte et par région	Pour toutes les conditions, à l'exception de la correspondance regex et de la correspondance géographique, 100 de chaque type de condition . Par exemple, 100 condition s de contraint e de taille et 100 condition s de correspon dance IP. Pour les conditions de regex et de géo-correspondance , consultez le tableau suivant.
Requêtes par seconde	25 000 par liste ACL web*

*Ce quota s'applique uniquement à AWS WAF Classic sur un Application Load Balancer. Les quotas de demandes par seconde (RPS) pour AWS WAF Classic on CloudFront sont les mêmes que ceux pris en charge par CloudFront les quotas RPS décrits dans le guide du CloudFront développeur.

Les quotas suivants sur les entités AWS WAF classiques ne peuvent pas être modifiés.

Ressource	Quota par compte et par région
Groupes de règles par liste ACL web	2 : 1 groupe de règles créé par le client et 1 AWS Marketplace groupe de règles
Règles par liste ACL web	10
Conditions par règle	10
Plages d'adresses IP (en notation CIDR) par condition de correspondance IP	10 000 Vous pouvez mettre à jour jusqu'à 1 000 adresses à la fois. L'appel d'API `UpdateIPSet` accepte un maximum de 1 000 adresses par requête.
Adresses IP bloquées par une règle basée sur un débit	10 000
Limite de débit pour une règle basée sur un débit par période de 5 minutes	100

Ressource	Quota par compte et par région
Filtre par condition de correspondance de scripts inter-site	10
Filtre par condition de contrainte de taille	10
Filtre par condition de correspondance d'injection SQL	10
Filtre par condition de correspondance de chaîne	10
Dans des conditions de correspondance de chaînes, le nombre de caractères dans les noms d'en-tête HTTP, lorsque vous avez configuré AWS WAF Classic pour inspecter les en-têtes des requêtes Web pour une valeur spécifiée	40
Dans des conditions de correspondance de chaîne, le nombre de caractères de la valeur que vous souhaitez que AWS WAF Classic recherche	50
Conditions de match Regex	10
Dans les conditions de correspondance regex, le nombre de caractères du modèle que vous souhaitez que AWS WAF Classic recherche	70
Dans les conditions de correspondance d'expressions régulières, le nombre de modèles par ensemble de modèles	10
Dans les conditions de correspondance d'expressions régulières, le nombre d'ensembles de modèles par condition d'expressions régulières	1
Ensembles de motifs	5
Conditions de match géographique	50
Emplacements par condition de correspondance géographique	50

AWS WAF Classic applique les quotas d'appels fixes suivants par compte et par région. Ces quotas s'appliquent au nombre total d'appels au service par tous les moyens disponibles, y compris la

console, la CLI AWS CloudFormation, l'API REST et les SDK. Ces quotas ne peuvent pas être modifiés.

Type d'appel	Quota par compte et par région
Nombre maximal d'appels à `AssociateWebACL`	1 demande toutes les 2 secondes
Nombre maximal d'appels à `DisassociateWebACL`	1 demande toutes les 2 secondes
Nombre maximal d'appels à `GetWebACLForResource`	1 demande par seconde
Nombre maximal d'appels à `ListResourcesForWebACL`	1 demande par seconde
Nombre maximal d'appels à `CreateWebACLMigrationStack`	1 demande par seconde
Nombre maximal d'appels à `GetChangeToken`	10 requêtes par seconde
Nombre maximal d'appels à `GetChangeTokenStatus`	1 demande par seconde
Nombre maximal d'appels à toute action `List` individuelle, si aucun autre quota n'est défini pour elle	5 demandes par seconde
Nombre maximal d'appels à toute action `Create`, `Put`, `Get` ou `Update` individuelle, si aucun autre quota n'est défini pour elle	1 demande par seconde

AWS Shield

La protection contre les attaques par déni de service distribué (DDoS) est d'une importance capitale pour vos applications connectées à Internet. Lorsque vous créez votre application AWS, vous pouvez utiliser les protections AWS fournies sans frais supplémentaires. En outre, vous pouvez utiliser le service AWS Shield Advanced géré de protection contre les menaces pour améliorer votre niveau de sécurité grâce à des fonctionnalités supplémentaires de détection, d'atténuation et de réponse aux attaques DDoS.

AWS s'engage à vous fournir les outils, les meilleures pratiques et les services nécessaires pour garantir une haute disponibilité, une sécurité et une résilience dans le cadre de votre défense contre les acteurs malveillants sur Internet. Ce guide est destiné à aider les décideurs informatiques et les ingénieurs en sécurité à comprendre comment utiliser Shield et Shield Advanced pour mieux protéger leurs applications contre les attaques DDoS et autres menaces externes.

Lorsque vous développez votre application AWS, vous bénéficiez d'une protection automatique AWS contre les vecteurs d'attaque DDoS volumétriques courants, tels que les attaques par réflexion UDP et les inondations TCP SYN. Vous pouvez tirer parti de ces protections pour garantir la disponibilité des applications sur lesquelles vous exécutez en concevant et AWS en configurant votre architecture pour garantir la résilience aux attaques DDoS.

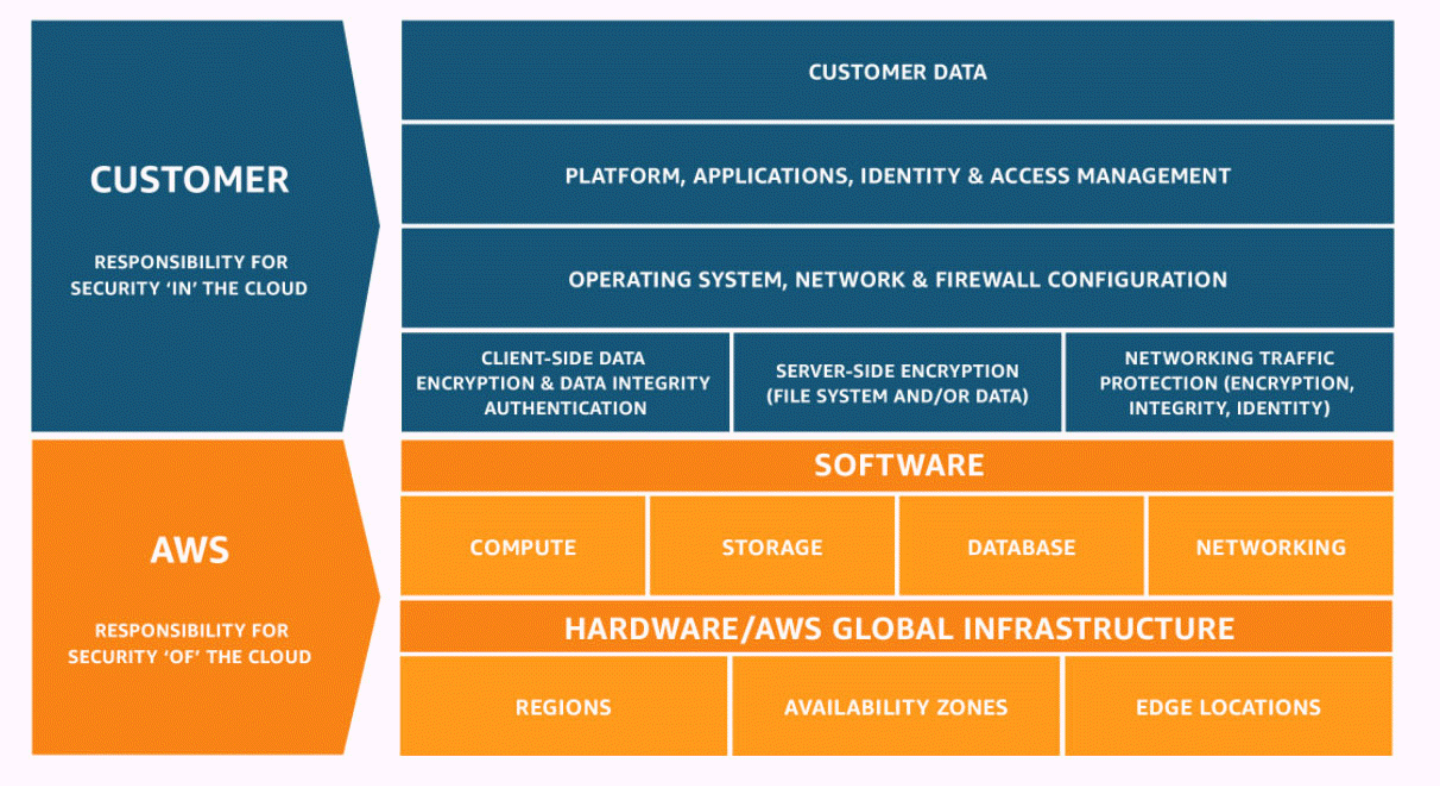
Ce guide fournit des recommandations qui peuvent vous aider à concevoir, créer et configurer vos architectures d'applications pour la résilience DDoS. Les applications qui respectent les meilleures pratiques décrites dans ce guide peuvent bénéficier d'une meilleure continuité de disponibilité lorsqu'elles sont ciblées par des attaques DDoS de plus grande envergure et par un éventail plus large de vecteurs d'attaques DDoS. En outre, ce guide explique comment utiliser Shield Advanced pour mettre en œuvre une posture de protection DDoS optimisée pour vos applications critiques. Il s'agit notamment des applications pour lesquelles vous avez garanti un certain niveau de disponibilité à vos clients et de celles qui nécessitent une assistance opérationnelle AWS lors d'événements DDoS.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. L'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers

dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Shield Advanced, consultez la section AWS Services concernés par le programme de conformité.

- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation ainsi que les lois et réglementations applicables.



Comment fonctionnent AWS Shield et Shield Advanced

AWS Shield Standard et AWS Shield Advanced fournissent des protections contre les attaques par déni de service distribué (DDoS) pour les AWS ressources des couches réseau et transport (couches 3 et 4) et de la couche application (couche 7). Une attaque DDoS est une attaque au cours de laquelle plusieurs systèmes compromis tentent d'inonder une cible de trafic. Une attaque DDoS peut empêcher les utilisateurs finaux légitimes d'accéder aux services cibles et provoquer le blocage de la cible en raison d'un volume de trafic écrasant.

AWS Shield fournit une protection contre un large éventail de vecteurs d'attaque DDoS connus et de vecteurs d'attaque zero-day. La détection et l'atténuation du Shield sont conçues pour fournir une couverture contre les menaces même si elles ne sont pas explicitement connues du service au

moment de la détection. Shield Standard est fourni automatiquement et sans frais supplémentaires lorsque vous l'utilisez AWS.

Les catégories d'attaques détectées par Shield sont les suivantes :

- Attaques volumétriques du réseau (couche 3) : il s'agit d'une sous-catégorie des vecteurs d'attaque de la couche d'infrastructure. Ces vecteurs tentent de saturer la capacité du réseau ou de la ressource ciblée, afin de refuser le service aux utilisateurs légitimes.
- Attaques de protocole réseau (couche 4) — Il s'agit d'une sous-catégorie de vecteurs d'attaque de couche d'infrastructure. Ces vecteurs abusent d'un protocole pour refuser le service à la ressource ciblée. Un exemple courant d'attaque de protocole réseau est l'inondation TCP SYN, qui peut épuiser l'état de connexion sur des ressources telles que les serveurs, les équilibreurs de charge ou les pare-feux. Une attaque de protocole réseau peut également être volumétrique. Par exemple, une inondation TCP SYN plus importante peut avoir pour but de saturer la capacité d'un réseau tout en épuisant l'état de la ressource ciblée ou des ressources intermédiaires.
- Attaques au niveau de l'application (couche 7) : cette catégorie de vecteurs d'attaque tente de refuser le service à des utilisateurs légitimes en inondant une application de requêtes valides pour la cible, telles que des inondations de requêtes Web.

Table des matières

- AWS Shield logique d'atténuation pour les AWS régions
- AWS Shield logique d'atténuation pour les accélérateurs AWS Global Accelerator standard
- AWS Shield Advanced logique d'atténuation pour les adresses IP élastiques
- AWS Shield Advanced logique d'atténuation pour les applications Web

AWS Shield Standard vue d'ensemble

AWS Shield est un service géré de protection contre les menaces qui protège le périmètre de votre application. Le périmètre est le premier point d'entrée pour le trafic applicatif provenant de l'extérieur du AWS réseau.

Pour déterminer le périmètre de votre application, considérez la manière dont les utilisateurs accèdent à votre application depuis Internet. Si le premier point d'entrée se trouve dans une AWS région, le périmètre de l'application est votre Amazon Virtual Private Cloud (VPC). Si les utilisateurs sont dirigés vers votre application par Amazon Route 53 et accèdent d'abord à l'application via Amazon CloudFront ou AWS Global Accelerator, le périmètre de l'application commence à la périphérie du AWS réseau.

Shield offre des avantages en matière de détection et d'atténuation des attaques DDoS pour toutes les applications qui s'exécutent AWS, mais les décisions que vous prenez lors de la conception de l'architecture de votre application influenceront votre niveau de résilience aux attaques DDoS. La résilience DDoS est la capacité de votre application à continuer à fonctionner selon les paramètres attendus lors d'une attaque.

Tous les AWS clients bénéficient de la protection automatique de Shield Standard, sans frais supplémentaires. Shield Standard protège contre les attaques DDoS les plus courantes et les plus fréquentes sur le réseau et la couche transport qui ciblent votre site Web ou vos applications. Shield Standard contribue à protéger tous les AWS clients, mais vous bénéficiez d'avantages particuliers grâce aux zones hébergées Amazon Route 53, aux CloudFront distributions Amazon et aux accélérateurs AWS Global Accelerator standard. Ces ressources bénéficient d'une protection de disponibilité complète contre toutes les attaques connues au niveau du réseau et de la couche de transport.

AWS Shield Advanced vue d'ensemble

AWS Shield Advanced est un service géré qui vous aide à protéger votre application contre les menaces externes, telles que les attaques DDoS, les bots volumétriques et les tentatives

d'exploitation de vulnérabilités. Pour les plus hauts niveaux de protection contre les attaques, vous pouvez vous abonner à AWS Shield Advanced.

Lorsque vous vous abonnez à Shield Advanced et que vous ajoutez une protection à vos ressources, Shield Advanced fournit une protection étendue contre les attaques DDoS pour ces ressources. Les protections que vous offre Shield Advanced peuvent varier en fonction de votre architecture et de vos choix de configuration. Utilisez les informations contenues dans ce guide pour créer et protéger des applications résilientes à l'aide de Shield Advanced, et pour monter en puissance lorsque vous avez besoin de l'aide d'un expert.

Abonnements et AWS WAF coûts de Shield Advanced

Votre abonnement Shield Advanced couvre les coûts liés à l'utilisation des AWS WAF fonctionnalités standard pour les ressources que vous protégez avec Shield Advanced. Les AWS WAF frais standard couverts par vos protections Shield Advanced sont le coût par ACL Web, le coût par règle et le prix de base par million de demandes d'inspection de requêtes Web, jusqu'à 1 500 WCU et jusqu'à la taille corporelle par défaut.

L'activation de l'atténuation automatique des attaques DDoS par la couche application Shield Advanced ajoute un groupe de règles à votre ACL Web qui utilise 150 unités de capacité ACL Web (WCU). Ces WCU sont pris en compte dans l'utilisation des WCU dans votre ACL Web. Pour plus d’informations, consultez Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative, Le groupe de règles Shield Advanced et AWS WAF unités de capacité ACL Web (WCU).

Votre abonnement à Shield Advanced ne couvre pas l'utilisation de AWS WAF ressources que vous ne protégez pas à l'aide de Shield Advanced. Il ne couvre pas non plus les AWS WAF coûts non standard supplémentaires liés aux ressources protégées. Des exemples de AWS WAF coûts non standard sont ceux liés au contrôle des robots, à l'action des CAPTCHA règles, aux ACL Web qui utilisent plus de 1 500 WCU et à l'inspection du corps de la demande au-delà de la taille par défaut. La liste complète est disponible sur la page de AWS WAF tarification.

Pour obtenir des informations complètes et des exemples de tarification, consultez Shield Pricing and AWS WAF Pricing.

Facturation de l'abonnement Shield Advanced

Si vous êtes revendeur de AWS chaînes, contactez l'équipe chargée de votre compte pour obtenir des informations et des conseils. Ces informations de facturation sont destinées aux clients qui ne sont pas des revendeurs de AWS canaux.

Pour tous les autres, les directives d'abonnement et de facturation suivantes s'appliquent :

- Pour les comptes membres d'une AWS Organizations organisation, facturez AWS les abonnements Shield Advanced sur le compte payeur de l'organisation, que le compte payeur lui-même soit souscrit ou non.
- Lorsque vous souscrivez plusieurs comptes appartenant à la même famille de comptes de facturation AWS Organizations consolidée, le prix d'abonnement unique couvre tous les comptes souscrits de la famille. L'organisation doit être propriétaire de Comptes AWS la totalité de ses ressources.
- Lorsque vous souscrivez plusieurs comptes pour plusieurs organisations, vous pouvez toujours payer les mêmes frais d'abonnement pour l'ensemble des organisations, des comptes et des ressources, à condition que vous les possédiez tous. Contactez votre responsable de compte ou le service d' AWS assistance et demandez une exemption des frais AWS Shield Advanced d'abonnement pour toutes les organisations sauf une.

Pour obtenir des informations détaillées sur les prix et des exemples, consultez la section AWS Shield Tarification.

Rubriques

- AWS Shield Advanced ressources protégées
- AWS Shield Advanced capacités et options
- Décider s'il convient de souscrire à des protections supplémentaires AWS Shield Advanced et d'appliquer des protections supplémentaires

AWS Shield Advanced ressources protégées

> **Note**
>
> Les protections Shield Advanced ne sont activées que pour les ressources que vous avez explicitement spécifiées dans Shield Advanced ou que vous protégez par le biais d'une politique AWS Firewall Manager Shield Advanced. Shield Advanced ne protège pas automatiquement vos ressources.

Vous pouvez utiliser Shield Advanced pour une surveillance et une protection avancées avec les types de ressources suivants :

- CloudFront Distributions Amazon. Pour CloudFront un déploiement continu, Shield Advanced protège toute distribution intermédiaire associée à une distribution principale protégée.
- Zones hébergées Amazon Route 53.
- AWS Global Accelerator accélérateurs standard.
- Adresses IP élastiques Amazon EC2. Shield Advanced protège les ressources associées aux adresses IP Elastic protégées.
- Instances Amazon EC2, par association à des adresses IP Amazon EC2 Elastic.
- Les équilibreurs de charge Elastic Load Balancing (ELB) suivants :
  - Équilibreurs de charge des applications.
  - Équilibreurs Classic Load Balancer.
  - Équilibreurs de charge réseau, via des associations aux adresses IP Amazon EC2 Elastic.

Pour plus d'informations sur les protections pour ces types de ressources, consultezAWS Shield Advanced protections par type de ressource.

AWS Shield Advanced capacités et options

AWS Shield Advanced l'abonnement inclut les fonctionnalités et options suivantes. Elles complètent les capacités de détection et d'atténuation des attaques DDoS dont vous bénéficiez déjà. AWS

- AWS WAF intégration — Shield Advanced utilise des ACL, des règles et des groupes de règles AWS WAF Web dans le cadre de ses protections de la couche application. Pour plus d'informations sur AWS WAF, voirComment AWS WAF fonctionne.

> **Note**
>
> Votre abonnement Shield Advanced couvre les coûts liés à l'utilisation des AWS WAF fonctionnalités standard pour les ressources que vous protégez avec Shield Advanced. Les AWS WAF frais standard couverts par vos protections Shield Advanced sont le coût par ACL Web, le coût par règle et le prix de base par million de demandes d'inspection de requêtes Web, jusqu'à 1 500 WCU et jusqu'à la taille corporelle par défaut. L'activation de l'atténuation automatique des attaques DDoS par la couche application Shield Advanced ajoute un groupe de règles à votre ACL Web qui utilise 150 unités de capacité ACL Web (WCU). Ces WCU sont pris en compte dans l'utilisation des WCU dans votre ACL Web. Pour plus d'informations, consultez Shield Advanced : atténuation

automatique des attaques DDoS au niveau de la couche applicative, Le groupe de règles Shield Advanced et AWS WAF unités de capacité ACL Web (WCU).

Votre abonnement à Shield Advanced ne couvre pas l'utilisation de AWS WAF ressources que vous ne protégez pas à l'aide de Shield Advanced. Il ne couvre pas non plus les AWS WAF coûts non standard supplémentaires liés aux ressources protégées. Des exemples de AWS WAF coûts non standard sont ceux liés au contrôle des robots, à l'action des CAPTCHA règles, aux ACL Web qui utilisent plus de 1 500 WCU et à l'inspection du corps de la demande au-delà de la taille par défaut. La liste complète est disponible sur la page de AWS WAF tarification.

Pour obtenir des informations complètes et des exemples de tarification, consultez Shield Pricing and AWS WAF Pricing.

- Atténuation automatique des attaques DDoS au niveau de l'application : vous pouvez configurer Shield Advanced pour qu'il réponde automatiquement afin d'atténuer les attaques au niveau de la couche application (couche 7) contre vos ressources protégées. Grâce à l'atténuation automatique, Shield Advanced impose une limite de AWS WAF débit aux demandes provenant de sources DDoS connues, et ajoute et gère automatiquement des AWS WAF protections personnalisées en réponse aux attaques DDoS détectées. Vous pouvez configurer l'atténuation automatique pour compter ou bloquer les requêtes Web qui font partie d'une attaque.

  Pour plus d'informations, consultez Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

- Détection basée sur l'état de santé : vous pouvez utiliser les contrôles de santé d'Amazon Route 53 avec Shield Advanced pour détecter et atténuer les événements. Les bilans de santé surveillent votre application conformément à vos spécifications, signalant qu'elle est saine lorsque vos spécifications sont respectées et qu'elle n'est pas saine lorsqu'elles ne le sont pas. L'utilisation de tests de santé avec Shield Advanced permet d'éviter les faux positifs et de détecter et d'atténuer plus rapidement les problèmes de santé d'une ressource protégée. Vous pouvez utiliser la détection basée sur l'état de santé pour tous les types de ressources, à l'exception des zones hébergées Route 53. L'engagement proactif de Shield Advanced n'est disponible que pour les ressources dont la détection basée sur l'état de santé est activée.

  Pour plus d'informations, consultez Détection basée sur l'état de santé au moyen de bilans.

- Groupes de protection : vous pouvez utiliser des groupes de protection pour créer des regroupements logiques de vos ressources protégées, afin d'améliorer la détection et l'atténuation du groupe dans son ensemble. Vous pouvez définir les critères d'appartenance à un groupe de

protection afin que les ressources nouvellement protégées soient automatiquement incluses. Une ressource protégée peut appartenir à plusieurs groupes de protection.

Pour plus d'informations, consultez AWS Shield Advanced groupes de protection.

- Visibilité améliorée sur les événements et les attaques DDoS : Shield Advanced vous donne accès à des statistiques et à des rapports avancés en temps réel pour une visibilité étendue des événements et des attaques visant vos AWS ressources protégées. Vous pouvez accéder à ces informations via l'API et la console Shield Advanced, ainsi que via Amazon CloudWatch Metrics.

  Pour plus d'informations, consultez Visibilité sur les événements DDoS.

- Gestion centralisée des protections Shield Advanced par AWS Firewall Manager : vous pouvez utiliser Firewall Manager pour appliquer automatiquement les protections Shield Advanced à vos nouveaux comptes et ressources et pour déployer des AWS WAF règles sur vos ACL Web. Les politiques de protection de Firewall Manager Shield Advanced sont incluses sans frais supplémentaires pour les clients de Shield Advanced. Vous pouvez également centraliser vos activités de surveillance Shield Advanced pour vos comptes en utilisant Firewall Manager avec une rubrique Amazon Simple Notification Service (SNS) ou. AWS Security Hub

  Pour plus d'informations sur l'utilisation de Firewall Manager pour gérer les protections Shield Advanced, consultez AWS Firewall Manager etAWS Shield Advanced politiques. Pour plus d'informations sur la tarification de Firewall Manager, consultez la section AWS Firewall Manager Tarification.

- AWS Shield Response Team (SRT) — La SRT possède une vaste expérience dans le domaine de la protection AWS d'Amazon.com et de ses filiales. En tant que AWS Shield Advanced client, vous pouvez contacter le SRT à tout moment pour obtenir de l'aide lors d'une attaque DDoS affectant la disponibilité de votre application. Vous pouvez également travailler avec le SRT pour créer et gérer des mesures d'atténuation personnalisées pour vos ressources. Pour utiliser les services du SRT, vous devez également être abonné au plan Business Support ou au plan Enterprise Support.

  Pour plus d'informations, consultez Assistance de la Shield Response Team (SRT).

- Engagement proactif : grâce à un engagement proactif, la Shield Response Team (SRT) vous contacte directement si le bilan de santé Amazon Route 53 que vous avez associé à votre ressource protégée ne fonctionne pas correctement lors d'un événement détecté par Shield Advanced. Cela vous permet de communiquer plus rapidement avec des experts lorsque la disponibilité de votre application est susceptible d'être affectée par une attaque présumée.

  Pour plus d'informations, consultez Configuration de l'engagement proactif.

- Opportunités de protection des coûts — Shield Advanced offre une certaine protection contre les pics de votre AWS facture qui pourraient résulter d'une attaque DDoS contre vos ressources protégées. Cela peut inclure une couverture en cas de hausse des frais d'utilisation du Shield Advanced data transfer out (DTO). Shield Advanced fournit une protection contre les coûts sous forme de crédits de service Shield Advanced.

  Pour plus d'informations, voir Demande de crédit en AWS Shield Advanced.

Décider s'il convient de souscrire à des protections supplémentaires AWS Shield Advanced et d'appliquer des protections supplémentaires

Consultez les scénarios décrits dans cette section pour vous aider à choisir les comptes auxquels vous souhaitez vous abonner AWS Shield Advanced et les domaines dans lesquels appliquer des protections supplémentaires. Avec Shield Advanced, vous payez un abonnement mensuel pour tous les comptes créés sous un compte de facturation consolidé, plus les frais d'utilisation basés sur le Go de données transférées. Pour plus d'informations sur les tarifs de Shield Advanced, consultez la section AWS Shield Advanced Tarification.

Pour protéger une application et ses ressources avec Shield Advanced, vous devez abonner les comptes qui gèrent l'application à Shield Advanced, puis vous ajoutez des protections aux ressources de l'application. Pour plus d'informations sur la souscription de comptes et la protection des ressources, consultezCommencer avec AWS Shield Advanced.

Abonnements et AWS WAF coûts de Shield Advanced

Votre abonnement Shield Advanced couvre les coûts liés à l'utilisation des AWS WAF fonctionnalités standard pour les ressources que vous protégez avec Shield Advanced. Les AWS WAF frais standard couverts par vos protections Shield Advanced sont le coût par ACL Web, le coût par règle et le prix de base par million de demandes d'inspection de requêtes Web, jusqu'à 1 500 WCU et jusqu'à la taille corporelle par défaut.

L'activation de l'atténuation automatique des attaques DDoS par la couche application Shield Advanced ajoute un groupe de règles à votre ACL Web qui utilise 150 unités de capacité ACL Web (WCU). Ces WCU sont pris en compte dans l'utilisation des WCU dans votre ACL Web. Pour plus d'informations, consultez Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative, Le groupe de règles Shield Advanced et AWS WAF unités de capacité ACL Web (WCU).

Votre abonnement à Shield Advanced ne couvre pas l'utilisation de AWS WAF ressources que vous ne protégez pas à l'aide de Shield Advanced. Il ne couvre pas non plus les AWS WAF coûts non standard supplémentaires liés aux ressources protégées. Des exemples de AWS WAF coûts non standard sont ceux liés au contrôle des robots, à l'action des CAPTCHA règles, aux ACL Web qui utilisent plus de 1 500 WCU et à l'inspection du corps de la demande au-delà de la taille par défaut. La liste complète est disponible sur la page de AWS WAF tarification.

Pour obtenir des informations complètes et des exemples de tarification, consultez Shield Pricing and AWS WAF Pricing.

Facturation de l'abonnement Shield Advanced

Si vous êtes revendeur de AWS chaînes, contactez l'équipe chargée de votre compte pour obtenir des informations et des conseils. Ces informations de facturation sont destinées aux clients qui ne sont pas des revendeurs de AWS canaux.

Pour tous les autres, les directives d'abonnement et de facturation suivantes s'appliquent :

- Pour les comptes membres d'une AWS Organizations organisation, facturez AWS les abonnements Shield Advanced sur le compte payeur de l'organisation, que le compte payeur lui-même soit souscrit ou non.
- Lorsque vous souscrivez plusieurs comptes appartenant à la même famille de comptes de facturation AWS Organizations consolidée, le prix d'abonnement unique couvre tous les comptes souscrits de la famille. L'organisation doit être propriétaire de Comptes AWS la totalité de ses ressources.
- Lorsque vous souscrivez plusieurs comptes pour plusieurs organisations, vous pouvez toujours payer les mêmes frais d'abonnement pour l'ensemble des organisations, des comptes et des ressources, à condition que vous les possédiez tous. Contactez votre responsable de compte ou le service d' AWS assistance et demandez une exemption des frais AWS Shield Advanced d'abonnement pour toutes les organisations sauf une.

Pour obtenir des informations détaillées sur les prix et des exemples, consultez la section AWS Shield Tarification.

Identification des applications à protéger

Envisagez de mettre en œuvre les protections Shield Advanced pour les applications où vous avez besoin de l'un des éléments suivants :

- Disponibilité garantie pour les utilisateurs de l'application.
- Accès rapide à des experts en atténuation des attaques DDoS si l'application est affectée par une attaque DDoS.
- Prise de conscience du AWS fait que l'application est susceptible d'être affectée par une attaque DDoS et notification des attaques par vos équipes chargées de la sécurité ou des opérations AWS et notification de leur escalade.
- La prévisibilité des coûts de votre cloud, y compris lorsqu'une attaque DDoS affecte votre utilisation des AWS services.

Si une application ou ses ressources nécessitent l'un des éléments ci-dessus, pensez à créer des abonnements pour les comptes associés.

Identifier les ressources à protéger

Pour chaque compte abonné, pensez à ajouter une protection Shield Advanced à chaque ressource présentant l'une des caractéristiques suivantes :

- La ressource est destinée aux utilisateurs externes sur Internet.
- La ressource est exposée à Internet et fait également partie d'une application critique. Tenez compte de chaque ressource exposée, que vous souhaitiez ou non qu'elle soit accessible aux utilisateurs sur Internet.
- La ressource est protégée par une ACL AWS WAF Web.

Pour en savoir plus sur la création et la gestion de protections pour vos ressources, consultezProtection des ressources dans AWS Shield Advanced.

En outre, suivez les recommandations de ce guide pour vous assurer que vous concevez votre application de manière à ce qu'elle soit résiliente aux attaques DDoS et que vous avez correctement configuré les fonctionnalités de Shield Advanced pour une protection optimale.

Exemples d'attaques DDoS

AWS Shield Advanced fournit une protection étendue contre de nombreux types d'attaques.

La liste suivante décrit certains types d'attaques courants :

Attaques par réflexion UDP (User Datagram Protocol)

Dans les attaques par réflexion UDP, un attaquant peut usurper la source d'une requête et utiliser le protocole UDP pour obtenir une réponse importante de la part du serveur. Le trafic réseau supplémentaire dirigé vers l'adresse IP usurpée et attaquée peut ralentir le serveur ciblé et empêcher les utilisateurs finaux légitimes d'accéder aux ressources nécessaires.

Inondation TCP SYN

Le but d'une attaque TCP SYN flood est d'épuiser les ressources disponibles d'un système en laissant les connexions dans un état semi-ouvert. Lorsqu'un utilisateur se connecte à un service TCP tel qu'un serveur Web, le client envoie un paquet TCP SYN. Le serveur retourne un accusé de réception et le client retourne son propre accusé de réception, ce qui termine la connexion en trois temps. Lors d'un afflux TCP SYN, le troisième accusé de réception n'est jamais renvoyé et le serveur attend une réponse. Cela peut empêcher d'autres utilisateurs de se connecter au serveur.

Inondation de requêtes DNS

Lors d'un afflux de requêtes DNS, un attaquant utilise plusieurs requêtes DNS pour épuiser les ressources d'un serveur DNS. AWS Shield Advanced peut aider à fournir une protection contre les attaques par inondation de requêtes DNS sur les serveurs DNS Route 53.

Attaques par Cache Busting/inondation HTTP (couche 7)

Dans le cas d'une inondation HTTP, y compris `GET` et `POST` d'une inondation, un attaquant envoie plusieurs requêtes HTTP qui semblent provenir d'un utilisateur réel de l'application Web. Les attaques par Cache Busting constituent un type d'inondation HTTP qui utilise des variations dans la chaîne de requête de la requête HTTP qui empêchent l'utilisation de contenu mis en cache sur un emplacement périphérique et qui forcent le contenu à être fourni à partir du serveur web d'origine, ce qui entraîne des contraintes supplémentaires et potentiellement dangereuses sur le serveur web d'origine.

Comment AWS Shield détecte les événements

AWS exploite des systèmes de détection de niveau de service pour le AWS réseau et les AWS services individuels, afin de garantir leur disponibilité lors d'une attaque DDoS. En outre, les systèmes de détection au niveau des ressources surveillent chaque AWS ressource individuelle pour s'assurer que le trafic vers la ressource reste dans les limites des paramètres attendus. Cette combinaison protège à la fois les AWS ressources et les AWS services ciblés, en appliquant des mesures d'atténuation qui suppriment les paquets défectueux connus, mettent en évidence le trafic potentiellement malveillant et hiérarchisent le trafic provenant des utilisateurs finaux.

Les événements détectés apparaissent dans les résumés des événements de votre Shield Advanced, les détails des attaques et CloudWatch les statistiques Amazon sous forme de nom du vecteur d'attaque DDoS ou comme `Volumetric` si l'évaluation était basée sur le volume de trafic plutôt que sur la signature. Pour plus d'informations sur les dimensions du vecteur d'attaque disponibles dans la `DDoSDetected` CloudWatch métrique, voir AWS Shield Advanced métriques

Rubriques

- Logique de détection des menaces pesant sur la couche d'infrastructure
- Logique de détection des menaces pesant sur la couche applicative
- Logique de détection pour plusieurs ressources dans une application

Logique de détection des menaces pesant sur la couche d'infrastructure

La logique de détection utilisée pour protéger les AWS ressources ciblées contre les attaques DDoS dans les couches d'infrastructure (couche 3 et couche 4) dépend du type de ressource et du fait que la ressource est protégée ou non. AWS Shield Advanced

Détection pour Amazon CloudFront et Amazon Route 53

Lorsque vous servez votre application Web avec CloudFront et Route 53, tous les paquets envoyés à l'application sont inspectés par un système d'atténuation des attaques DDoS entièrement intégré, qui n'introduit aucune latence observable. Les attaques DDoS contre les CloudFront distributions et les zones hébergées par Route 53 sont atténuées en temps réel. Ces protections s'appliquent indépendamment du fait que vous les utilisiez ou non AWS Shield Advanced.

Suivez les meilleures pratiques en utilisant CloudFront Route 53 comme point d'entrée de votre application Web dans la mesure du possible pour détecter et atténuer les événements DDoS le plus rapidement possible.

Détection pour AWS Global Accelerator les services régionaux

La détection au niveau des ressources protège les accélérateurs et les ressources AWS Global Accelerator standard lancés dans les AWS régions, tels que les équilibreurs de charge classiques, les équilibreurs de charge d'application et les adresses IP élastiques (EIP). Ces types de ressources sont surveillés pour détecter les élévations de trafic susceptibles d'indiquer la présence d'une attaque DDoS nécessitant une atténuation. Chaque minute, le trafic vers chaque AWS ressource est évalué. Si le trafic vers une ressource est élevé, des contrôles supplémentaires sont effectués pour mesurer la capacité de la ressource.

Shield effectue les contrôles standard suivants :

- Instances Amazon Elastic Compute Cloud (Amazon EC2), EIP associées aux instances Amazon EC2 — Shield récupère la capacité de la ressource protégée. La capacité dépend du type d'instance cible, de la taille de l'instance et d'autres facteurs tels que le fait que l'instance utilise ou non une mise en réseau améliorée.
- Équilibreurs de charge classiques et équilibreurs de charge d'application : Shield récupère la capacité du nœud d'équilibreur de charge ciblé.
- EIP connectés aux équilibreurs de charge réseau — Shield récupère la capacité de l'équilibreur de charge ciblé. La capacité est indépendante de la configuration de groupe de l'équilibreur de charge cible.
- AWS Global Accelerator accélérateurs standard — Shield récupère la capacité, qui est basée sur la configuration du terminal.

Ces évaluations portent sur plusieurs dimensions du trafic réseau, telles que le port et le protocole. Si la capacité de la ressource ciblée est dépassée, Shield met en place une solution d'atténuation des attaques DDoS. Les mesures d'atténuation mises en place par Shield réduiront le trafic DDoS, mais ne l'élimineront peut-être pas. Shield peut également mettre en place une mesure d'atténuation si une fraction de la capacité de la ressource est dépassée sur une dimension de trafic compatible avec les vecteurs d'attaque DDoS connus. Shield applique à cette atténuation une durée de vie limitée (TTL), qu'elle prolonge tant que l'attaque est en cours.

> **Note**
>
> Les mesures d'atténuation mises en place par Shield réduiront le trafic DDoS, mais ne l'élimineront peut-être pas. Vous pouvez compléter Shield avec des solutions telles AWS Network Firewall qu'un pare-feu sur l'hôte, iptables afin d'empêcher votre application de traiter le trafic qui n'est pas valide pour votre application ou qui n'a pas été généré par des utilisateurs finaux légitimes.

Les protections Shield Advanced ajoutent les éléments suivants aux activités de détection Shield existantes :

- Seuils de détection inférieurs — Shield Advanced place les mesures d'atténuation à la moitié de la capacité calculée. Cela permet d'atténuer plus rapidement les attaques qui s'intensifient lentement et d'atténuer les attaques dont la signature volumétrique est plus ambiguë.

- Protection contre les attaques intermittentes — Shield Advanced propose des mesures d'atténuation liées à l'augmentation exponentielle de la durée de vie (TTL), en fonction de la fréquence et de la durée des attaques. Cela permet de maintenir les mesures d'atténuation en place plus longtemps lorsqu'une ressource est fréquemment ciblée et lorsqu'une attaque se produit en rafales brèves.
- Détection basée sur l'état de santé : lorsque vous associez un bilan de santé Route 53 à une ressource protégée par Shield Advanced, l'état du bilan de santé est utilisé dans la logique de détection. Lors d'un événement détecté, si le bilan de santé est correct, Shield Advanced doit être plus sûr qu'il s'agit d'une attaque avant de mettre en place une mesure d'atténuation. Si, au contraire, le bilan de santé n'est pas satisfaisant, Shield Advanced peut mettre en place une mesure d'atténuation avant même que la confiance ne soit établie. Cette fonctionnalité permet d'éviter les faux positifs et de réagir plus rapidement aux attaques qui affectent votre application. Pour plus d'informations sur les contrôles de santé réalisés avec Shield Advanced, consultezDétection basée sur l'état de santé au moyen de bilans.

Logique de détection des menaces pesant sur la couche applicative

AWS Shield Advanced fournit une détection de la couche d'application Web pour les CloudFront distributions Amazon protégées et les équilibreurs de charge d'application. Lorsque vous protégez ces types de ressources avec Shield Advanced, vous pouvez associer une ACL AWS WAF Web à votre protection pour permettre la détection de la couche d'application Web. Shield Advanced utilise les données de demande pour l'ACL Web associée et crée une base de trafic pour votre application. La détection de la couche d'application Web repose sur l'intégration native entre Shield Advanced et AWS WAF. Pour en savoir plus sur les protections de la couche application, notamment sur l'association d'une ACL AWS WAF Web à une ressource protégée Shield Advanced, consultezAWS Shield Advanced protections de la couche d'application (couche 7).

Pour la détection de la couche d'application Web, Shield Advanced surveille le trafic des applications et le compare aux lignes de base historiques à la recherche d'anomalies. Cette surveillance couvre le volume total et la composition du trafic. Lors d'une attaque DDoS, nous nous attendons à ce que le volume et la composition du trafic changent, et Shield Advanced exige un écart statistiquement significatif dans les deux cas pour déclarer un événement.

Shield Advanced effectue ses mesures par rapport à des fenêtres temporelles historiques. Cette approche permet de réduire les notifications faussement positives résultant de modifications légitimes du volume de trafic ou de modifications du trafic correspondant à un schéma attendu, comme une vente proposée à la même heure chaque jour.

> **Note**
>
> Évitez les faux positifs dans vos protections Shield Advanced en laissant à Shield Advanced le temps d'établir des bases de référence représentant des modèles de trafic normaux et légitimes. Shield Advanced commence à collecter des informations pour sa base de référence lorsque vous associez une ACL Web à votre ressource protégée. Associez une ACL Web à votre ressource protégée au moins 24 heures avant tout événement planifié susceptible de provoquer des modèles inhabituels dans votre trafic Web. La détection de la couche d'application Web Shield Advanced est plus précise lorsqu'elle a observé 30 jours de trafic normal.

Le temps nécessaire à Shield Advanced pour détecter un événement dépend de l'ampleur des changements observés dans le volume de trafic. Pour les variations de volume plus faibles, Shield Advanced observe le trafic pendant une période plus longue, afin de s'assurer qu'un événement se produit. En cas de variations de volume plus importantes, Shield Advanced détecte et signale un événement plus rapidement.

Une règle basée sur le taux dans votre ACL Web, qu'elle soit ajoutée par vous-même ou par la fonction d'atténuation automatique de la couche d'application Shield Advanced, peut atténuer une attaque avant qu'elle n'atteigne un niveau détectable. Pour plus d'informations sur l'atténuation automatique des attaques DDoS au niveau de la couche application, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

> **Note**
>
> Vous pouvez concevoir votre application de manière à ce qu'elle évolue en réponse à un trafic ou à une charge élevés afin de garantir qu'elle ne soit pas affectée par de faibles volumes de demandes. Avec Shield Advanced, vos ressources protégées sont couvertes par une protection des coûts. Cela vous permet de vous protéger contre les augmentations inattendues de votre facture cloud qui pourraient survenir à la suite d'une attaque DDoS. Pour en savoir plus sur la protection des coûts Shield Advanced, consultezDemande de crédit en AWS Shield Advanced.

Logique de détection pour plusieurs ressources dans une application

Vous pouvez utiliser AWS Shield Advanced des groupes de protection pour créer des ensembles de ressources protégées faisant partie de la même application. Vous pouvez choisir les ressources protégées à placer dans un groupe ou indiquer que toutes les ressources du même type doivent être traitées comme un seul groupe. Par exemple, vous pouvez créer un groupe de tous les équilibreurs de charge d'application. Lorsque vous créez un groupe de protection, la détection Shield Advanced agrège tout le trafic des ressources protégées au sein du groupe. Cela est utile si vous disposez de nombreuses ressources qui ont chacune un faible volume de trafic, mais avec un volume agrégé important. Vous pouvez également utiliser des groupes de protection pour préserver les lignes de base des applications, dans le cas de déploiements bleu-vert où le trafic est transféré entre des ressources protégées.

Vous pouvez choisir d'agréger le trafic au sein de votre groupe de protection de l'une des manières suivantes :

- Somme : cette agrégation combine l'ensemble du trafic entre les ressources du groupe de protection. Vous pouvez utiliser cette agrégation pour garantir que les ressources nouvellement créées disposent d'une base de référence existante et pour réduire la sensibilité de détection, ce qui permet d'éviter les faux positifs.
- Moyenne : cette agrégation utilise la moyenne de l'ensemble du trafic au sein du groupe de protection. Vous pouvez utiliser cette agrégation pour les applications où le trafic entre les ressources est uniforme, comme les équilibreurs de charge.
- Max : cette agrégation utilise le trafic le plus élevé de toutes les ressources du groupe de protection. Vous pouvez utiliser cette agrégation lorsqu'il existe plusieurs niveaux d'une application dans un groupe de protection. Par exemple, vous pouvez avoir un groupe de protection qui inclut une CloudFront distribution, son origine d'Application Load Balancer et les cibles d'instance Amazon EC2 de l'Application Load Balancer.

Vous pouvez également utiliser des groupes de protection pour améliorer la vitesse à laquelle Shield Advanced met en place des mesures d'atténuation, en cas d'attaques ciblant plusieurs adresses IP élastiques ou AWS Global Accelerator des accélérateurs standard connectés à Internet. Lorsqu'une ressource d'un groupe de protection est ciblée, Shield Advanced établit la confiance des autres ressources du groupe. Cela met la détection Shield Advanced en alerte et peut réduire le temps nécessaire pour créer des mesures d'atténuation supplémentaires.

Pour en savoir plus sur les groupes de protection, consultezAWS Shield Advanced groupes de protection.

Comment AWS Shield atténuer les événements

La logique d'atténuation qui protège votre application peut varier en fonction de l'architecture de votre application. Lorsque vous protégez une application Web avec Amazon CloudFront et Amazon Route 53, vous bénéficiez de mesures d'atténuation spécifiques aux cas d'utilisation du Web et du DNS et qui protègent l'ensemble du trafic lié aux services. Lorsque le point d'entrée de votre application est une ressource qui s'exécute dans une AWS région, la logique d'atténuation varie en fonction du service, du type de ressource et de l'utilisation que vous en faites AWS Shield Advanced.

AWS Les systèmes d'atténuation des attaques DDoS sont développés par les ingénieurs de Shield et sont étroitement intégrés aux AWS services. Les ingénieurs prennent en compte les aspects de votre architecture tels que la capacité et l'état des ressources ciblées. Les ingénieurs de Shield surveillent en permanence l'efficacité et les performances des systèmes d'atténuation des attaques DDoS et sont en mesure de réagir rapidement lorsque de nouvelles menaces sont découvertes ou anticipées.

Vous pouvez concevoir votre application de manière à ce qu'elle évolue en réponse à un trafic ou à une charge élevés, afin de garantir qu'elle ne soit pas affectée par de faibles volumes de demandes. Si vous utilisez Shield Advanced pour protéger vos ressources, vous bénéficiez d'une couverture contre les augmentations inattendues de votre facture cloud qui pourraient survenir à la suite d'une attaque DDoS.

Atténuations liées aux infrastructures

Pour les attaques au niveau de l'infrastructure, des systèmes d'atténuation des attaques AWS Shield DDoS sont présents à la frontière du AWS réseau et aux emplacements AWS périphériques. La mise en place de plusieurs niveaux de contrôles de sécurité dans l'ensemble de l' AWS infrastructure fournit defense-in-depth à vos applications cloud.

Shield gère des systèmes d'atténuation des attaques DDoS à tous les points d'entrée depuis Internet. Lorsque Shield détecte une attaque DDoS, pour chaque point d'entrée, il redirige le trafic via les systèmes d'atténuation des attaques DDoS situés au même endroit. Cela n'introduit aucune latence supplémentaire observable et fournit une capacité d'atténuation de plus de TeraBits 100 Tbit/s dans toutes les AWS régions et tous les emplacements périphériques. Shield protège la disponibilité de vos ressources sans rediriger le trafic vers des centres de nettoyage externes ou distants, ce qui pourrait augmenter la latence.

- À la frontière du AWS réseau, quel que soit le AWS service ou la ressource, les systèmes d'atténuation des attaques DDoS atténuent les attaques au niveau de l'infrastructure provenant d'Internet. Les systèmes effectuent leurs mesures d'atténuation lorsqu'ils sont signalés par le système de détection du Shield ou par un ingénieur de la Shield Response Team (SRT).
- Sur les sites AWS périphériques, les systèmes d'atténuation des attaques DDoS inspectent en permanence chaque paquet transféré vers les CloudFront distributions Amazon et les zones hébergées Amazon Route 53, quelle que soit son origine. Au besoin, les systèmes appliquent des mesures d'atténuation spécifiquement conçues pour le trafic Web et DNS. Un autre avantage de l'utilisation d'Amazon CloudFront et d'Amazon Route 53 pour protéger vos applications Web est que les attaques DDoS sont immédiatement atténuées, sans qu'un signal de détection de Shield ne soit nécessaire.

Atténuations de la couche applicative

Shield Advanced fournit des mesures d'atténuation de la couche d'application Web pour les CloudFront distributions Amazon et les équilibreurs de charge d'application pour lesquels vous avez activé les protections Shield Advanced. Lorsque vous activez la protection, vous associez une ACL AWS WAF Web à la ressource afin de permettre la détection de la couche d'application Web. En outre, vous avez la possibilité d'activer l'atténuation automatique de la couche d'application, qui demande à Shield Advanced de gérer les protections pour vous lors d'une attaque DDoS.

Shield fournit uniquement des mesures d'atténuation personnalisées pour les attaques de la couche application sur les ressources pour lesquelles vous avez activé Shield Advanced et l'atténuation automatique de la couche application. Grâce à l'atténuation automatique, Shield Advanced impose une limite de AWS WAF débit aux demandes provenant de sources DDoS connues, et ajoute et gère automatiquement des AWS WAF protections personnalisées en réponse aux attaques DDoS détectées. Pour des informations détaillées sur les mesures d'atténuation de ce type, consultezComment Shield Advanced gère l'atténuation automatique.

Une règle basée sur le taux dans votre ACL Web, qu'elle soit ajoutée par vous-même ou par la fonctionnalité d'atténuation automatique de la couche d'application Shield Advanced, peut atténuer une attaque avant qu'elle n'atteigne un niveau détectable. Pour plus d'informations sur la détection, consultezLogique de détection des menaces pesant sur la couche applicative.

Caractéristiques d'atténuation

Les principales caractéristiques de l'atténuation des AWS Shield attaques DDoS sont les suivantes :

- Validation des paquets — Cela garantit que chaque paquet inspecté est conforme à une structure attendue et est valide pour son protocole. Les validations de protocole prises en charge incluent IP, TCP (y compris l'en-tête et les options), UDP, ICMP, DNS et NTP.
- Listes de contrôle d'accès (ACL) et shapers : une ACL évalue le trafic par rapport à des attributs spécifiques et supprime le trafic correspondant ou le mappe à un shaper. Le shaper limite le débit de paquets pour le trafic correspondant, en supprimant les paquets excédentaires afin de contenir le volume qui atteint la destination. AWS Shield les ingénieurs de détection et de Shield Response Team (SRT) peuvent fournir des allocations de débit dédiées au trafic attendu et des allocations de débit plus restrictives au trafic dont les attributs correspondent aux vecteurs d'attaque DDoS connus. Les attributs auxquels une ACL peut correspondre incluent le port, le protocole, les indicateurs TCP, l'adresse de destination, le pays source et les modèles arbitraires de la charge utile du paquet.
- Notation de suspicion — Cela utilise les connaissances que Shield possède du trafic attendu pour appliquer un score à chaque paquet. Les paquets qui suivent de plus près les modèles de trafic dont on sait qu'ils sont bons se voient attribuer un score de suspicion inférieur. L'observation d'attributs de trafic défectueux connus peut augmenter le score de suspicion d'un paquet. Lorsqu'il est nécessaire de limiter le débit des paquets, Shield supprime d'abord les paquets présentant des scores de suspicion plus élevés. Cela permet à Shield d'atténuer à la fois les attaques DDoS connues et les attaques DDoS de type « jour zéro », tout en évitant les faux positifs.
- Proxy TCP SYN : il fournit une protection contre les inondations TCP SYN en envoyant des cookies TCP SYN pour contester les nouvelles connexions avant de les autoriser à passer au service protégé. Le proxy TCP SYN fourni par Shield DDoS mitigation est apatride, ce qui lui permet d'atténuer les plus grandes attaques TCP SYN connues sans atteindre l'état d'épuisement. Ceci est réalisé en intégrant les AWS services pour transférer l'état de connexion au lieu de maintenir un proxy continu entre le client et le service protégé. Le proxy TCP SYN est actuellement disponible sur Amazon et CloudFront Amazon Route 53.
- Distribution du débit — Cela ajuste en permanence les valeurs du shaper par emplacement en fonction du schéma d'entrée du trafic vers une ressource protégée. Cela permet d'éviter de limiter le débit du trafic client susceptible de ne pas pénétrer uniformément sur le AWS réseau.

AWS Shield logique d'atténuation pour CloudFront et Route 53

Shield DDoS Mitigation inspecte en permanence le trafic pour la Route CloudFront 53. Ces services fonctionnent à partir d'un réseau mondial d'emplacements AWS périphériques qui vous offrent un accès étendu à la capacité d'atténuation des attaques DDoS de Shield et fournissent votre application à partir d'une infrastructure plus proche de vos utilisateurs finaux.

- CloudFront— Les mesures d'atténuation des attaques DDoS du Shield autorisent uniquement le trafic valide pour les applications Web à accéder au service. Cela fournit une protection automatique contre de nombreux vecteurs DDoS courants, tels que les attaques par réflexion UDP.

  CloudFront maintient des connexions persistantes avec l'origine de votre application, les inondations TCP SYN sont automatiquement atténuées grâce à l'intégration avec la fonctionnalité proxy Shield TCP SYN, et le protocole TLS (Transport Layer Security) est interrompu à la périphérie. Ces fonctionnalités combinées garantissent que l'origine de votre application ne reçoit que des requêtes Web bien formulées et qu'elle est protégée contre les attaques DDoS de niveau inférieur, les inondations de connexions et les abus du TLS.

  CloudFront utilise une combinaison de direction du trafic DNS et de routage anycast. Ces techniques améliorent la résilience de votre application en atténuant les attaques à proximité de la source, en isolant les défaillances et en garantissant l'accès aux capacités nécessaires pour atténuer les plus importantes attaques connues.
- Les mesures d'atténuation de Route 53 — Shield autorisent uniquement les requêtes DNS valides à atteindre le service. Shield atténue le flot de requêtes DNS grâce à un score de suspicion qui donne la priorité aux requêtes dont on sait qu'elles sont valides et ne donne plus la priorité aux requêtes contenant des attributs d'attaque DDoS suspects ou connus.

  Route 53 utilise le shuffle sharding pour fournir un ensemble unique de quatre adresses IP de résolution à chaque zone hébergée, pour IPv4 et IPv6. Chaque adresse IP correspond à un sous-ensemble différent d'emplacements Route 53. Chaque sous-ensemble de localisation est constitué de serveurs DNS officiels qui ne recouvrent que partiellement l'infrastructure de tout autre sous-ensemble. Cela garantit que si une requête utilisateur échoue pour une raison quelconque, elle sera traitée avec succès lors d'une nouvelle tentative.

  Route 53 utilise le routage anycast pour diriger les requêtes DNS vers l'emplacement périphérique le plus proche, en fonction de la proximité du réseau. Anycast répartit également le trafic DDoS vers de nombreux emplacements périphériques, ce qui empêche les attaques de se concentrer sur un seul emplacement.

Outre la rapidité de l'atténuation, CloudFront Route 53 fournit un accès étendu à la capacité distribuée à l'échelle mondiale de Shield. Pour tirer parti de ces fonctionnalités, utilisez ces services comme point d'entrée de vos applications Web dynamiques ou statiques.

Pour en savoir plus sur l'utilisation CloudFront de Route 53 pour protéger les applications Web, consultez Comment protéger les applications Web dynamiques contre les attaques DDoS en utilisant

Amazon CloudFront et Amazon Route 53. Pour en savoir plus sur l'isolation des défauts sur la Route 53, consultez une étude de cas sur l'isolation globale des défauts.

AWS Shield logique d'atténuation pour les AWS régions

Les ressources lancées dans les AWS régions sont protégées par des systèmes d'atténuation des AWS Shield attaques DDoS placés par le système de détection au niveau des ressources de Shield. Les ressources régionales incluent les adresses IP élastiques (EIP), les équilibreurs de charge classiques et les équilibreurs de charge d'application.

Avant de mettre en place une mesure d'atténuation, Shield identifie la ressource ciblée et sa capacité. Shield utilise cette capacité pour déterminer le trafic total maximal que ses mesures d'atténuation devraient permettre de transférer vers la ressource. Les listes de contrôle d'accès (ACL) et les autres shapers inclus dans le cadre de l'atténuation peuvent réduire les volumes autorisés pour certains trafics, par exemple le trafic correspondant à des vecteurs d'attaque DDoS connus ou dont le volume n'est pas censé être important. Cela limite davantage le volume de trafic autorisé par les mesures d'atténuation pour les attaques par réflexion UDP ou pour le trafic TCP doté d'indicateurs TCP SYN ou FIN.

Shield détermine la capacité et place les mesures d'atténuation différemment pour chaque type de ressource.

- Pour une instance Amazon EC2 ou une EIP attachée à une instance Amazon EC2, Shield calcule la capacité en fonction du type d'instance et d'autres attributs de l'instance, par exemple si la mise en réseau améliorée est activée sur l'instance.
- Pour un Application Load Balancer ou un Classic Load Balancer, Shield calcule la capacité individuellement pour chaque nœud cible de l'équilibreur de charge. L'atténuation des attaques DDoS pour ces ressources est assurée par une combinaison de mesures d'atténuation des attaques DDoS du Shield et d'une mise à l'échelle automatique par l'équilibreur de charge. Lorsque la Shield Response Team (SRT) est engagée dans une attaque contre une ressource Application Load Balancer ou Classic Load Balancer, elle peut accélérer le dimensionnement comme mesure de protection supplémentaire.
- Shield calcule la capacité de certaines AWS ressources en fonction de la capacité disponible de l' AWS infrastructure sous-jacente. Ces types de ressources incluent les équilibreurs de charge réseau (NLB) et les ressources qui acheminent le trafic via des équilibreurs de charge de passerelle ou. AWS Network Firewall

> **Note**
>
> Protégez vos équilibreurs de charge réseau en connectant des EIP protégés par Shield Advanced. Vous pouvez travailler avec SRT pour créer des mesures d'atténuation personnalisées basées sur le trafic attendu et la capacité de l'application sous-jacente.

Lorsque Shield met en place une mesure d'atténuation, les limites de taux initiales définies par Shield dans la logique d'atténuation sont appliquées de la même manière à tous les systèmes d'atténuation DDoS de Shield. Par exemple, si Shield place une atténuation avec une limite de 100 000 paquets par seconde (pps), il autorisera initialement 100 000 pps sur chaque site. Shield agrège ensuite en permanence les mesures d'atténuation pour déterminer le ratio réel de trafic, et utilise ce ratio pour adapter la limite de débit pour chaque site. Cela permet d'éviter les faux positifs et de garantir que les mesures d'atténuation ne sont pas trop permissives.

AWS Shield logique d'atténuation pour les accélérateurs AWS Global Accelerator standard

Les mesures d'atténuation du Shield permettent uniquement au trafic valide d'atteindre les points de terminaison d'un accélérateur standard Global Accelerator. Les accélérateurs standard sont déployés dans le monde entier et vous fournissent des adresses IP que vous pouvez utiliser pour acheminer le trafic vers les AWS ressources de n'importe quelle AWS région. Les limites de débit appliquées par Shield pour atténuer les effets des accélérateurs mondiaux sont basées sur les capacités des ressources vers lesquelles l'accélérateur standard achemine le trafic. Shield met en place des mesures d'atténuation lorsque le trafic total dépasse le débit déterminé, et également lorsqu'une fraction de ce taux est dépassée pour les vecteurs DDoS connus.

Lorsque vous configurez un accélérateur standard, vous définissez des groupes de points de terminaison pour chaque AWS région dans laquelle vous acheminerez le trafic pour votre application. Lorsque Shield place une mesure d'atténuation, il calcule la capacité de chaque groupe de terminaux et met à jour les limites de débit de chaque système d'atténuation DDoS du Shield en conséquence. Le tarif varie pour chaque emplacement, en fonction des hypothèses formulées par Shield quant à la manière dont le trafic sera acheminé d'Internet vers vos AWS ressources. La capacité d'un groupe de points de terminaison est calculée comme le nombre de ressources du groupe multiplié par la capacité la plus faible de toutes les ressources du groupe. À intervalles réguliers, Shield recalcule la capacité de votre application et met à jour les limites de débit selon les besoins.

> **Note**
>
> L'utilisation de cadrans de trafic pour modifier le pourcentage du trafic dirigé vers un groupe de terminaux ne change pas la façon dont Shield calcule ou distribue les limites de débit à ses systèmes d'atténuation des attaques DDoS. Si vous utilisez des numéros de trafic, configurez vos groupes de points de terminaison pour qu'ils se reflètent mutuellement en termes de type et de quantité de ressources. Cela permet de garantir que la capacité calculée par Shield est représentative des ressources qui acheminent le trafic pour votre application.

Pour plus d'informations sur les groupes de points de terminaison et les numéros de trafic dans Global Accelerator, consultez la section Groupes de points de terminaison dans les accélérateurs AWS Global Accelerator standard.

AWS Shield Advanced logique d'atténuation pour les adresses IP élastiques

Lorsque vous protégez une adresse IP élastique (EIP) avec AWS Shield Advanced, Shield Advanced améliore les mesures d'atténuation mises en place par Shield lors d'un événement DDoS. Les systèmes d'atténuation DDoS Shield Advanced répliquent la configuration Network ACL (NACL) pour le sous-réseau public auquel l'EIP est associé. Par exemple, si votre NACL est configurée pour bloquer tout le trafic UDP, Shield Advanced fusionne cette règle dans les mesures d'atténuation mises en place par Shield.

Cette fonctionnalité supplémentaire peut vous aider à éviter les risques de disponibilité liés à un trafic non valide pour votre application. Vous pouvez également utiliser les NACL pour bloquer des adresses IP sources individuelles ou des plages CIDR d'adresses IP sources. Cela peut être un outil d'atténuation utile pour les attaques DDoS qui ne sont pas distribuées. Il vous permet également de gérer facilement vos propres listes d'autorisations ou de bloquer les adresses IP qui ne devraient pas communiquer avec votre application, sans l'intervention d' AWS ingénieurs.

AWS Shield Advanced logique d'atténuation pour les applications Web

AWS Shield Advanced utilisés AWS WAF pour atténuer les attaques contre la couche applicative Web. AWS WAF est inclus dans Shield Advanced sans frais supplémentaires.

Protection standard de la couche d'application

Lorsque vous protégez une CloudFront distribution Amazon ou une Application Load Balancer avec Shield Advanced, vous pouvez utiliser Shield Advanced pour associer une ACL AWS WAF Web à

votre ressource protégée, si ce n'est pas déjà fait. Si vous n'avez pas encore configuré d'ACL Web, vous pouvez utiliser l'assistant de console Shield Advanced pour en créer une et y ajouter une règle basée sur le taux. Une règle basée sur le taux limite le nombre de demandes par fenêtre de cinq minutes pour chaque adresse IP, fournissant ainsi des protections de base contre les inondations de demandes au niveau de la couche application Web. Vous pouvez configurer le taux en commençant par 100. Pour plus d'informations, consultez Shield Advanced, couche d'application, ACL AWS WAF Web et règles basées sur le débit.

Vous pouvez également utiliser le AWS WAF service pour gérer l'ACL Web. Vous pouvez ainsi étendre la configuration de l'ACL Web pour inspecter des composants de requêtes Web spécifiques pour détecter des correspondances ou des modèles de chaînes, ajouter un traitement personnalisé des demandes et des réponses et les comparer à la géolocalisation de l'origine de la demande. AWS WAF Pour plus d'informations sur AWS WAF les règles, consultezAWS WAF règles.

Atténuation automatique des couches applicatives

Pour une protection améliorée, activez l'atténuation automatique de la couche d'application Shield Advanced. Avec cette option, Shield Advanced maintient une règle de limitation du AWS WAF débit pour les demandes provenant de sources DDoS connues et fournit des mesures d'atténuation personnalisées en cas d'attaques DDoS détectées.

Lorsque Shield Advanced détecte une attaque contre une ressource protégée, il tente d'identifier une signature d'attaque qui isole le trafic d'attaque du trafic normal vers votre application. Shield Advanced évalue la signature d'attaque identifiée par rapport aux modèles de trafic historiques pour la ressource attaquée, ainsi que pour toute autre ressource associée à la même ACL Web.

Si Shield Advanced détermine que la signature d'attaque isole uniquement le trafic impliqué dans l'attaque DDoS, il implémente la signature dans des AWS WAF règles au sein de l'ACL Web associée. Vous pouvez demander à Shield Advanced de mettre en place des mesures d'atténuation qui ne prennent en compte que le trafic auquel il correspond ou qui le bloque, et vous pouvez modifier le paramètre à tout moment. Lorsque Shield Advanced détermine que ses règles d'atténuation ne sont plus nécessaires, il les supprime de l'ACL Web. Pour plus d'informations sur l'atténuation des événements au niveau de la couche application, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

Pour plus d'informations sur les mesures d'atténuation de la couche d'application Shield Advanced, consultezAWS Shield Advanced protections de la couche d'application (couche 7).

Exemples d'architectures résilientes aux attaques DDoS de base

La résilience DDoS est la capacité de l'architecture de votre application à résister aux attaques par déni de service distribué (DDoS) tout en continuant à servir les utilisateurs finaux légitimes. Une application hautement résiliente peut rester disponible pendant une attaque avec un impact minimal sur les indicateurs de performance tels que les erreurs ou la latence. Cette section présente quelques exemples d'architectures courants et décrit comment utiliser les fonctionnalités de détection et d'atténuation des attaques DDoS fournies par AWS Shield Advanced pour améliorer leur résilience aux attaques DDoS.

Les exemples d'architectures présentés dans cette section mettent en évidence les AWS services qui offrent les meilleurs avantages en termes de résilience aux attaques DDoS pour vos applications déployées. Les avantages des services mis en avant sont les suivants :

- Accès à une capacité réseau distribuée dans le monde entier — Les services Amazon CloudFront et Amazon Route 53 vous permettent d'accéder à Internet et à des capacités d'atténuation des attaques DDoS sur le réseau périphérique AWS mondial. AWS Global Accelerator Cela est utile pour atténuer les attaques volumétriques de plus grande envergure, qui peuvent atteindre des térabits. Vous pouvez exécuter votre application dans n'importe quelle AWS région et utiliser ces services pour protéger la disponibilité et optimiser les performances pour vos utilisateurs légitimes.
- Protection contre les vecteurs d'attaque DDoS de la couche application Web — Il est préférable de limiter les attaques DDoS de la couche application Web en combinant l'échelle de l'application et un pare-feu d'application Web (WAF). Shield Advanced utilise les journaux d'inspection des requêtes Web AWS WAF pour détecter les anomalies qui peuvent être atténuées automatiquement ou via un engagement avec l'équipe de réponse du AWS Shield (SRT). L'atténuation automatique est disponible par le biais de règles AWS WAF basées sur le taux déployées et également par le biais de l'atténuation automatique des attaques DDoS au niveau de la couche d'application Shield Advanced.

En plus de passer en revue ces exemples, consultez et suivez les meilleures pratiques applicables dans la section AWS Meilleures pratiques pour la résilience des attaques DDoS.

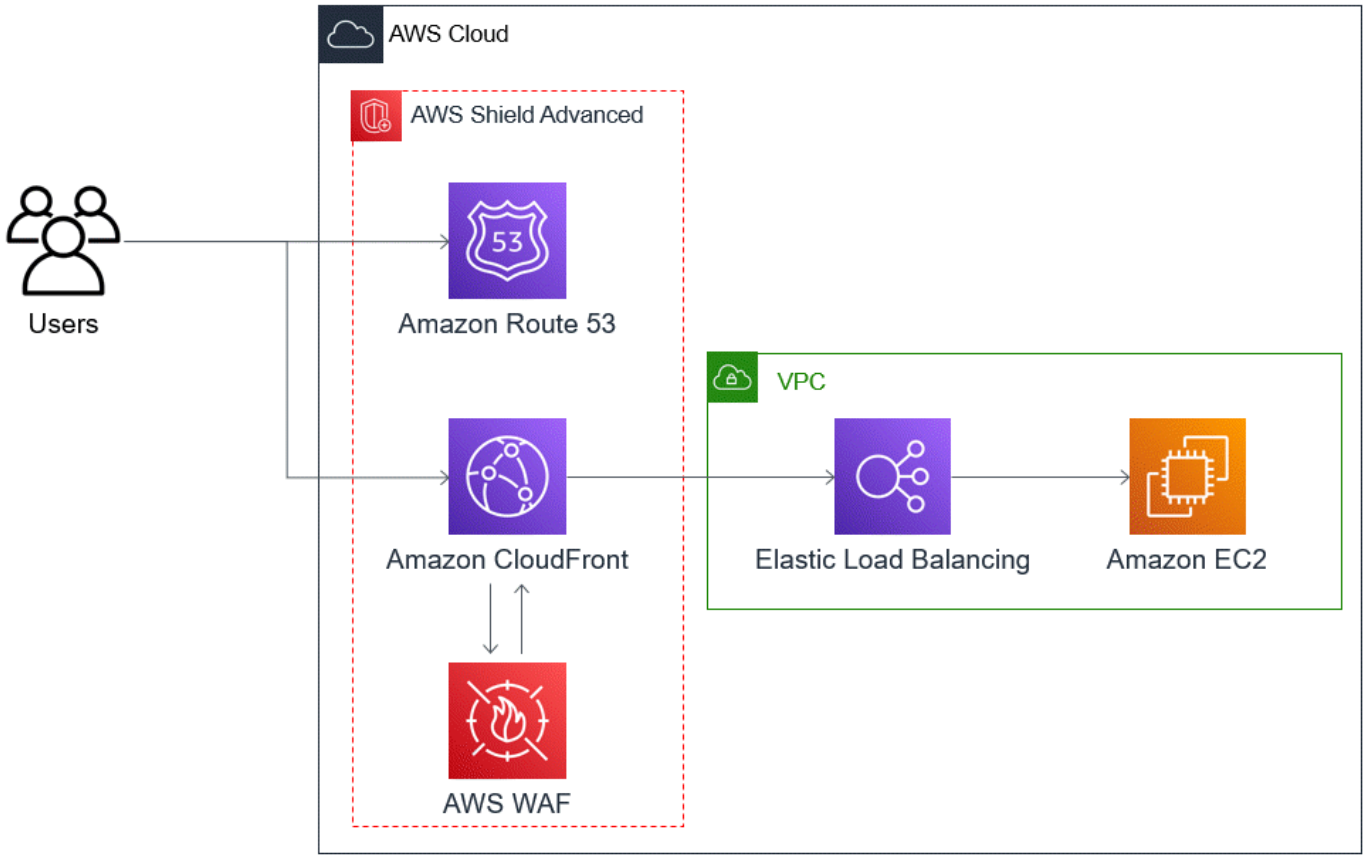
Exemple de résilience DDoS pour les applications Web courantes

Vous pouvez créer une application Web dans n'importe quelle AWS région et bénéficier d'une protection automatique contre les attaques DDoS grâce aux fonctionnalités de détection et d'atténuation AWS proposées dans la région.

Cet exemple concerne les architectures qui acheminent les utilisateurs vers une application Web à l'aide de ressources telles que les Classic Load Balancers, les Application Load Balancers, les Network Load Balancers, les solutions AWS Marketplace ou votre propre couche proxy. Vous pouvez améliorer la résilience DDoS en insérant des zones hébergées Amazon Route 53, des distributions CloudFront Amazon AWS WAF et des ACL Web entre ces ressources d'applications Web et vos utilisateurs. Ces insertions peuvent masquer l'origine de l'application, traiter les demandes au plus près de vos utilisateurs finaux et détecter et atténuer les inondations de demandes au niveau de la couche application. Les applications qui diffusent du contenu statique ou dynamique à vos utilisateurs avec Route 53 sont protégées par un système d'atténuation des attaques DDoS intégré CloudFront et entièrement intégré qui atténue les attaques au niveau de l'infrastructure en temps réel.

Une fois ces améliorations architecturales mises en place, vous pouvez protéger vos zones hébergées par Route 53 et vos CloudFront distributions avec Shield Advanced. Lorsque vous protégez CloudFront des distributions, Shield Advanced vous invite à associer des ACL AWS WAF Web et à créer des règles basées sur le taux pour celles-ci, et vous donne la possibilité d'activer l'atténuation automatique des attaques DDoS au niveau de la couche application ou un engagement proactif. L'engagement proactif et l'atténuation automatique des attaques DDoS au niveau de l'application utilisent les contrôles de santé Route 53 que vous associez à la ressource. Pour en savoir plus sur ces options, consultez Protection des ressources dans AWS Shield Advanced.

Le schéma de référence suivant décrit cette architecture résiliente aux attaques DDoS pour une application Web.



Les avantages que cette approche apporte à votre application Web sont les suivants :

- Protection contre les attaques DDoS fréquemment utilisées au niveau de l'infrastructure (couche 3 et couche 4), sans délai de détection. En outre, si une ressource est fréquemment ciblée, Shield Advanced applique des mesures d'atténuation pendant de plus longues périodes. Shield Advanced utilise également le contexte d'application déduit des ACL réseau (NACL) pour bloquer le trafic indésirable en amont. Cela permet d'isoler les défaillances au plus près de leur source, minimisant ainsi l'effet sur les utilisateurs légitimes.
- Protection contre les inondations TCP SYN. Les systèmes d'atténuation des attaques DDoS qui sont intégrés à CloudFront Route 53 et AWS Global Accelerator fournissent une fonctionnalité de proxy TCP SYN qui défie les nouvelles tentatives de connexion et ne sert que les utilisateurs légitimes.
- Protection contre les attaques de la couche applicative du DNS, car Route 53 est chargée de fournir des réponses DNS faisant autorité.

- Protection contre les inondations de demandes au niveau de la couche applicative Web. La règle basée sur le débit que vous configurez dans votre ACL AWS WAF Web bloque les adresses IP sources lorsqu'elles envoient plus de demandes que ce que la règle autorise.
- Atténuation automatique des attaques DDoS au niveau de la couche application pour vos CloudFront distributions, si vous choisissez d'activer cette option. Grâce à l'atténuation automatique des attaques DDoS, Shield Advanced maintient une règle basée sur le taux dans l'ACL AWS WAF Web associée à la distribution, qui limite le volume de demandes provenant de sources DDoS connues. En outre, lorsque Shield Advanced détecte un événement qui affecte l'état de votre application, il crée, teste et gère automatiquement des règles d'atténuation dans l'ACL Web.
- Engagement proactif avec la Shield Response Team (SRT), si vous choisissez d'activer cette option. Lorsque Shield Advanced détecte un événement qui affecte l'état de santé de votre application, le SRT répond et communique de manière proactive avec vos équipes chargées de la sécurité ou des opérations en utilisant les informations de contact que vous fournissez. Le SRT analyse les tendances de votre trafic et peut mettre à jour vos AWS WAF règles pour bloquer l'attaque.

Exemple de résilience DDoS pour les applications TCP et UDP

Cet exemple montre une architecture résiliente aux attaques DDoS pour les applications TCP et UDP dans une AWS région qui utilise des instances Amazon Elastic Compute Cloud (Amazon EC2) ou des adresses IP élastiques (EIP).

Vous pouvez suivre cet exemple général pour améliorer la résilience DDoS pour les types d'applications suivants :

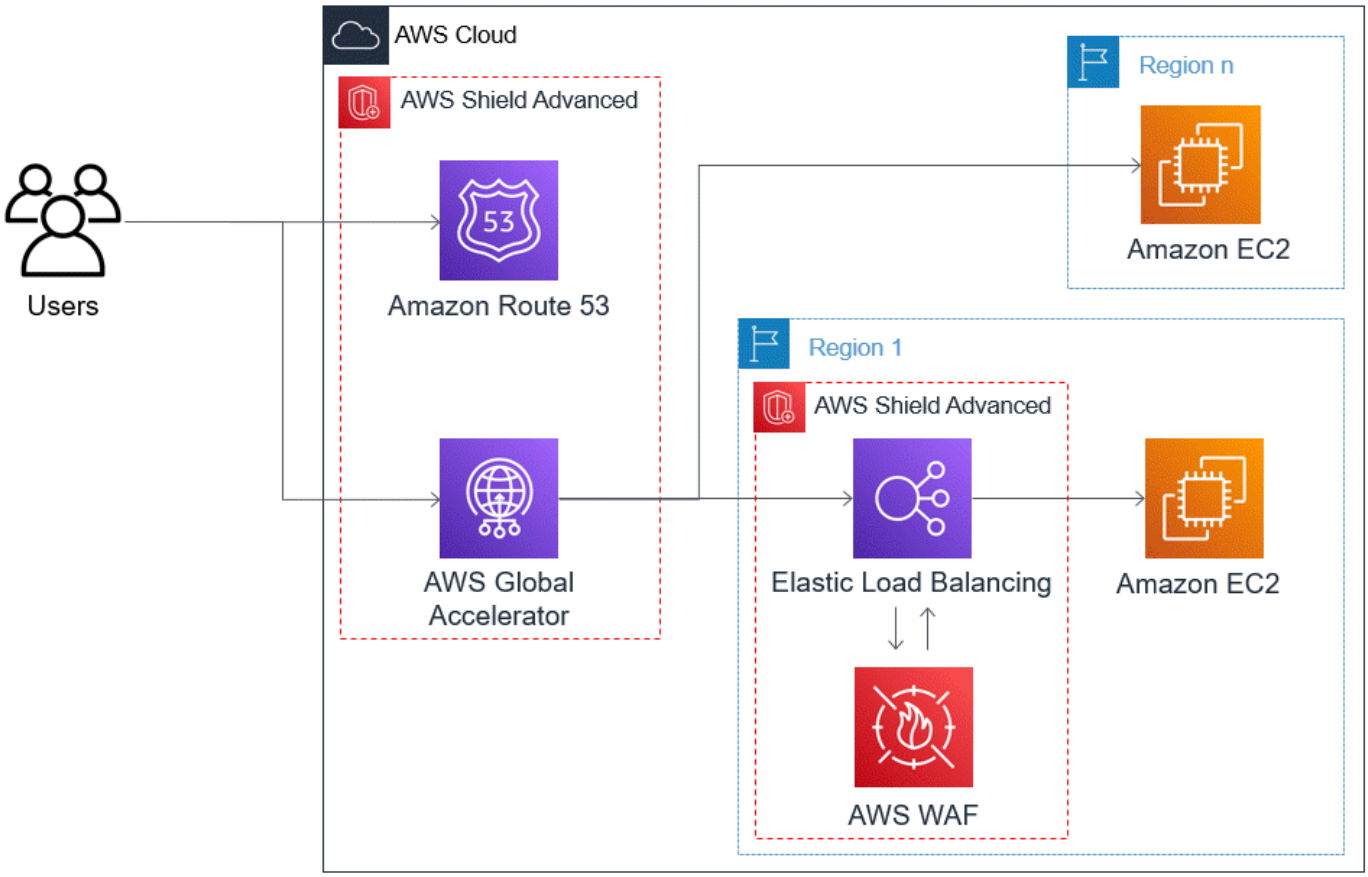
- Applications TCP ou UDP. Par exemple, les applications utilisées pour les jeux, l'IoT et la voix sur IP.
- Applications Web qui nécessitent des adresses IP statiques ou qui utilisent des protocoles non pris CloudFront en charge par Amazon. Par exemple, votre application peut avoir besoin d'adresses IP que vos utilisateurs peuvent ajouter à leurs listes d'autorisation de pare-feu et qui ne sont utilisées par aucun autre AWS client.

Vous pouvez améliorer la résilience DDoS pour ces types d'applications en introduisant Amazon Route 53 et. AWS Global Accelerator Ces services peuvent rediriger les utilisateurs vers votre application et fournir à celle-ci des adresses IP statiques qui sont acheminées de manière anycast

sur le réseau périphérique AWS mondial. Les accélérateurs standard de Global Accelerator peuvent améliorer la latence des utilisateurs jusqu'à 60 %. Si vous possédez une application Web, vous pouvez détecter et atténuer les inondations de demandes au niveau de la couche d'application Web en exécutant l'application sur un Application Load Balancer, puis en le protégeant à l'aide AWS WAF d'une ACL Web.

Après avoir créé votre application, protégez vos zones hébergées Route 53, les accélérateurs standard de Global Accelerator et tous les équilibreurs de charge d'application avec Shield Advanced. Lorsque vous protégez vos équilibreurs de charge d'application, vous pouvez associer des ACL AWS WAF Web et créer des règles basées sur le taux pour eux. Vous pouvez configurer un engagement proactif avec le SRT à la fois pour vos accélérateurs standard Global Accelerator et pour vos équilibreurs de charge d'application en associant des bilans de santé Route 53 nouveaux ou existants. Pour en savoir plus sur les options, voirProtection des ressources dans AWS Shield Advanced.

Le schéma de référence suivant décrit un exemple d'architecture résiliente aux attaques DDoS pour les applications TCP et UDP.



Les avantages que cette approche apporte à votre application sont les suivants :

- Protection contre les attaques DDoS de la plus grande couche d'infrastructure connue (couche 3 et couche 4). Si le volume d'une attaque provoque une congestion en amont AWS, la panne sera isolée plus près de sa source et aura un impact minimisé sur vos utilisateurs légitimes.
- Protection contre les attaques de la couche application DNS, car Route 53 est chargée de fournir des réponses DNS faisant autorité.
- Si vous avez une application Web, cette approche fournit une protection contre les inondations de demandes au niveau de la couche d'application Web. La règle basée sur le débit que vous configurez dans votre ACL AWS WAF Web bloque les adresses IP sources lorsqu'elles envoient plus de demandes que ce que la règle autorise.
- Engagement proactif avec la Shield Response Team (SRT), si vous choisissez d'activer cette option pour les ressources éligibles. Lorsque Shield Advanced détecte un événement qui affecte l'état de santé de votre application, le SRT répond et communique de manière proactive avec vos équipes chargées de la sécurité ou des opérations en utilisant les informations de contact que vous fournissez.

Exemples de cas d'utilisation de Shield Advanced

Vous pouvez utiliser Shield Advanced pour protéger vos ressources dans de nombreux types de scénarios. Cependant, dans certains cas, vous devez utiliser d'autres services ou combiner d'autres services avec Shield Advanced pour offrir la meilleure protection. Vous trouverez ci-dessous des exemples d'utilisation de Shield Advanced ou d'autres AWS services pour protéger vos ressources.

Objectif	Services suggérés	Documentation du service relatif
Protégez une application Web et les API RESTful contre une attaque DDoS	Shield Advanced protège une CloudFront distribution Amazon et un Application Load Balancer	Documentation sur Elastic Load Balancing, CloudFront documentation Amazon
Protège une application basée sur TCP contre une attaque DDoS	Shield Advanced protège un accélérateur AWS Global Accelerator standard ; associé à une adresse IP élastique	AWS Global Accelerator Documentation, documentation Elastic Load Balancing

Objectif	Services suggérés	Documentation du service relatif
Protège un serveur de jeu basé sur UDP contre une attaque DDoS	Shield Advanced protège une instance Amazon EC2 attachée à une adresse IP élastique	Documentation Amazon Elastic Compute Cloud

Par exemple, si vous utilisez Shield Advanced pour protéger une adresse IP élastique, Shield Advanced protège les ressources qui y sont associées. Lors d'une attaque, Shield Advanced déploie automatiquement les ACL de votre réseau jusqu'à la limite du AWS réseau. Lorsque les ACL de votre réseau se situent à la limite du réseau, Shield Advanced peut fournir une protection contre les événements DDoS plus importants. Généralement, les ACL réseau sont appliquées à proximité de vos instances Amazon EC2 au sein de votre Amazon VPC. L'ACL réseau ne peut atténuer les attaques que dans la mesure où votre VPC Amazon et votre instance peuvent les gérer. Si l'interface réseau attachée à votre instance Amazon EC2 peut traiter jusqu'à 10 Gbit/s, les volumes supérieurs à 10 Gbit/s ralentissent et bloquent éventuellement le trafic vers cette instance. Lors d'une attaque, Shield Advanced promeut l'ACL de votre réseau jusqu'à la AWS frontière, qui peut traiter plusieurs téraoctets de trafic. Votre ACL réseau est capable de fournir une protection pour votre ressource bien au-delà de la capacité typique de votre réseau. Pour plus d'informations sur les listes ACL réseau, consultez Listes ACL réseau.

Commencer avec AWS Shield Advanced

Ce didacticiel vous explique comment commencer à AWS Shield Advanced utiliser la console Shield Advanced.

> **Note**
>
> Shield Advanced nécessite un abonnement, ce qui n' AWS Shield Standard est pas le cas. Les protections fournies par Shield Standard sont disponibles gratuitement pour tous les AWS clients.

Shield Advanced fournit une protection avancée en matière de détection et d'atténuation des attaques DDoS pour les attaques de la couche réseau (couche 3), de la couche transport (couche 4)

et de la couche application (couche 7). Pour plus d'informations sur Shield Advanced, consultezAWS Shield Advanced vue d'ensemble.

La communauté AWS technique a publié un exemple de processus automatisé de configuration de Shield Advanced à l'aide des outils d'infrastructure en tant que code (IaC) AWS CloudFormation et de Terraform. Vous pouvez utiliser AWS Firewall Manager cette solution si vos comptes font partie d'une organisation AWS Organizations et si vous protégez des types de ressources, à l'exception d'Amazon Route 53 ou AWS Global Accelerator. Pour explorer cette option, consultez le référentiel de code sur aws-samples/ aws-shield-advanced-one-click-deployment et le didacticiel sur le déploiement en un clic de Shield Advanced.

> **Note**
>
> Il est important de configurer complètement Shield Advanced avant un événement de déni de service distribué (DDoS). Terminez la configuration pour vous assurer que votre application est protégée et que vous êtes prêt à réagir si votre application est affectée par une attaque DDoS.

Effectuez les étapes suivantes dans l'ordre pour commencer à utiliser Shield Advanced.

Table des matières

Abonnez-vous à AWS Shield Advanced

Vous devez vous abonner à Shield Advanced pour chaque produit Compte AWS que vous souhaitez protéger. Il n'est pas nécessaire de s'abonner à Shield Standard.

Facturation de l'abonnement Shield Advanced

Si vous êtes revendeur de AWS chaînes, contactez l'équipe chargée de votre compte pour obtenir des informations et des conseils. Ces informations de facturation sont destinées aux clients qui ne sont pas des revendeurs de AWS canaux.

Pour tous les autres, les directives d'abonnement et de facturation suivantes s'appliquent :

- Pour les comptes membres d'une AWS Organizations organisation, facturez AWS les abonnements Shield Advanced sur le compte payeur de l'organisation, que le compte payeur lui-même soit souscrit ou non.
- Lorsque vous souscrivez plusieurs comptes appartenant à la même famille de comptes de facturation AWS Organizations consolidée, le prix d'abonnement unique couvre tous les comptes souscrits de la famille. L'organisation doit être propriétaire de Comptes AWS la totalité de ses ressources.
- Lorsque vous souscrivez plusieurs comptes pour plusieurs organisations, vous pouvez toujours payer les mêmes frais d'abonnement pour l'ensemble des organisations, des comptes et des ressources, à condition que vous les possédiez tous. Contactez votre responsable de compte ou le service d' AWS assistance et demandez une exemption des frais AWS Shield Advanced d'abonnement pour toutes les organisations sauf une.

Pour obtenir des informations détaillées sur les prix et des exemples, consultez la section AWS Shield Tarification.

Simplifiez les abonnements avec AWS Firewall Manager

Si vos comptes font partie d'une organisation, nous vous recommandons de les utiliser AWS Firewall Manager , dans la mesure du possible, pour automatiser vos abonnements et vos protections pour l'organisation. Firewall Manager prend en charge tous les types de ressources protégées, à l'exception d'Amazon Route 53 et AWS Global Accelerator. Pour utiliser Firewall Manager, reportez-vous AWS Firewall Manager aux sections etCommencer à utiliser les AWS Firewall ManagerAWS Shield Advanced politiques.

Si vous n'utilisez pas Firewall Manager, pour chaque compte disposant de ressources nécessaires à la protection, abonnez-vous et ajoutez des protections en suivant les procédures suivantes.

Pour créer un compte auprès de AWS Shield Advanced

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

2. Dans la barre AWS Shieldde navigation, choisissez Getting started. Choisissez Subscribe to Shield Advanced.
3. Sur la page Subscribe to Shield Advanced, lisez chaque terme du contrat, puis cochez toutes les cases pour indiquer que vous acceptez les termes. Pour les comptes appartenant à une famille de facturation consolidée, vous devez accepter les conditions de chaque compte.

   > **Important**
   >
   > Lorsque vous êtes inscrit, pour vous désinscrire, vous devez contacter AWS Support. Pour désactiver le renouvellement automatique de votre abonnement, vous devez utiliser l'opération Shield API ou UpdateSubscriptionla commande CLI update-subscription.

   Choisissez Subscribe to Shield Advanced. Cela permet d'abonner votre compte à Shield Advanced et d'activer le service.

Votre compte est inscrit. Suivez les étapes suivantes pour protéger les ressources de votre compte avec Shield Advanced.

> **Note**
>
> Shield Advanced ne protège pas automatiquement vos ressources une fois que vous vous êtes abonné. Vous devez spécifier les ressources que Shield Advanced doit protéger et configurer les protections.

Ajoutez des ressources pour protéger et configurer les protections

Shield Advanced protège uniquement les ressources que vous spécifiez, soit par le biais de Shield Advanced, soit dans le cadre d'une politique Firewall Manager Shield Advanced. Il ne protège pas automatiquement les ressources d'un compte abonné.

Si vous utilisez une politique AWS Firewall Manager Shield Advanced pour vos protections, vous n'avez pas besoin de suivre cette étape. Vous configurez la politique avec les types de ressources à protéger, et Firewall Manager ajoute automatiquement des protections aux ressources couvertes par la politique.

Si vous n'utilisez pas Firewall Manager, suivez les procédures suivantes pour chaque compte disposant de ressources à protéger.

Pour choisir les ressources à protéger à l'aide de Shield Advanced

1. Choisissez Ajouter des ressources à protéger sur la page de confirmation d'abonnement de la procédure précédente, sur la page Ressources protégées ou sur la page Aperçu.
2. Sur la page Choisissez les ressources à protéger avec Shield Advanced, dans Spécifiez la région et les types de ressources, indiquez les spécifications de région et de type de ressource pour les ressources que vous souhaitez protéger. Vous pouvez protéger les ressources de plusieurs régions en sélectionnant Toutes les régions et vous pouvez restreindre la sélection aux ressources mondiales en sélectionnant Global. Vous pouvez désélectionner les types de ressources que vous ne souhaitez pas protéger. Pour plus d'informations sur les protections de vos types de ressources, consultezAWS Shield Advanced protections par type de ressource.
3. Choisissez Charger les ressources. Shield Advanced renseigne la section Select Resources avec les AWS ressources correspondant à vos critères.
4. Dans la section Sélectionner les ressources, vous pouvez filtrer la liste des ressources en saisissant une chaîne à rechercher dans les listes de ressources.

   Sélectionnez les ressources que vous souhaitez protéger.
5. Dans la section Tags, si vous souhaitez ajouter des balises aux protections Shield Advanced que vous créez, spécifiez-les. Pour plus d'informations sur le balisage AWS des ressources, consultez la section Utilisation de l'éditeur de balises.
6. Choisissez Protect with Shield Advanced. Cela ajoute les protections Shield Advanced aux ressources.

Parcourez les écrans de l'assistant de console pour terminer la configuration de la protection de vos ressources.

Rubriques

- Configurez les protections DDoS de la couche application (couche 7) avec AWS WAF
- Configurez la détection basée sur l'état de santé pour vos protections
- Configuration des alarmes et des notifications
- Vérifiez et finalisez votre configuration de protection

Configurez les protections DDoS de la couche application (couche 7) avec AWS WAF

Pour protéger une ressource de la couche application, Shield Advanced utilise une ACL AWS WAF Web avec une règle basée sur le débit comme point de départ. AWS WAF est un pare-feu d'applications Web qui vous permet de surveiller les requêtes HTTP et HTTPS qui sont transmises aux ressources de la couche application et de contrôler l'accès à votre contenu en fonction des caractéristiques des demandes. Une règle basée sur le débit limite le volume de trafic en fonction de vos critères d'agrégation des demandes, fournissant ainsi une protection DDoS de base à votre application. Pour plus d'informations, consultez Comment AWS WAF fonctionne et Instruction de règle basée sur un taux.

Vous pouvez également activer l'atténuation automatique des attaques DDoS au niveau de la couche application de Shield Advanced, afin que Shield Advanced limite le débit des demandes provenant de sources DDoS connues et vous fournisse automatiquement des protections spécifiques aux incidents.

> **Important**
>
> Si vous gérez vos protections Shield Advanced à AWS Firewall Manager l'aide d'une politique Shield Advanced, vous ne pouvez pas gérer les protections de la couche application ici. Vous devez les gérer dans votre politique Firewall Manager Shield Advanced.

Abonnements et AWS WAF coûts de Shield Advanced

Votre abonnement Shield Advanced couvre les coûts liés à l'utilisation des AWS WAF fonctionnalités standard pour les ressources que vous protégez avec Shield Advanced. Les AWS WAF frais standard couverts par vos protections Shield Advanced sont le coût par ACL Web, le coût par règle et le prix de base par million de demandes d'inspection de requêtes Web, jusqu'à 1 500 WCU et jusqu'à la taille corporelle par défaut.

L'activation de l'atténuation automatique des attaques DDoS par la couche application Shield Advanced ajoute un groupe de règles à votre ACL Web qui utilise 150 unités de capacité ACL Web (WCU). Ces WCU sont pris en compte dans l'utilisation des WCU dans votre ACL Web. Pour plus d'informations, consultez Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative, Le groupe de règles Shield Advanced et AWS WAF unités de capacité ACL Web (WCU).

Votre abonnement à Shield Advanced ne couvre pas l'utilisation de AWS WAF ressources que vous ne protégez pas à l'aide de Shield Advanced. Il ne couvre pas non plus les AWS WAF coûts non standard supplémentaires liés aux ressources protégées. Des exemples de AWS WAF coûts non standard sont ceux liés au contrôle des robots, à l'action des CAPTCHA règles, aux ACL Web qui utilisent plus de 1 500 WCU et à l'inspection du corps de la demande au-delà de la taille par défaut. La liste complète est disponible sur la page de AWS WAF tarification.

Pour obtenir des informations complètes et des exemples de tarification, consultez Shield Pricing and AWS WAF Pricing.

Pour configurer les protections DDoS de couche 7 pour une région

Shield Advanced vous donne la possibilité de configurer l'atténuation des attaques DDoS de couche 7 pour chaque région où se trouvent les ressources que vous avez choisies. Si vous ajoutez des protections dans plusieurs régions, l'assistant vous explique la procédure suivante pour chaque région.

1. La page Configurer les protections DDoS de la couche 7 répertorie chaque ressource qui n'est pas encore associée à une ACL Web. Pour chacune d'entre elles, choisissez une ACL Web existante ou créez une nouvelle ACL Web. Pour toute ressource qui possède déjà une ACL Web associée, vous pouvez modifier les ACL Web en dissociant d'abord la liste ACL actuelle. AWS WAF Pour plus d'informations, consultez Associer ou dissocier une ACL Web à une ressource AWS.

   Pour les ACL Web qui n'ont pas encore de règle basée sur le taux, l'assistant de configuration vous invite à en ajouter une. Une règle basée sur le débit limite le trafic provenant des adresses IP lorsque celles-ci envoient un volume élevé de demandes. Les règles basées sur le débit aident à protéger votre application contre les inondations de requêtes Web et peuvent fournir des alertes en cas de pics de trafic soudains susceptibles d'indiquer une attaque DDoS potentielle. Ajoutez une règle basée sur le taux à une ACL Web en choisissant Ajouter une règle de limite de débit, puis en fournissant une limite de débit et une action de règle. Vous pouvez configurer des protections supplémentaires dans l'ACL Web via AWS WAF.

   Pour plus d'informations sur l'utilisation des ACL Web et des règles basées sur le taux dans vos protections Shield Advanced, y compris des options de configuration supplémentaires pour les règles basées sur le taux, consultez. Shield Advanced, couche d'application, ACL AWS WAF Web et règles basées sur le débit
2. Pour l'atténuation automatique des attaques DDoS au niveau de la couche application, si vous souhaitez que Shield Advanced atténue automatiquement les attaques DDoS contre les

ressources de votre couche application, choisissez Enable, puis sélectionnez l'action de AWS WAF règle que vous souhaitez que Shield Advanced utilise dans ses règles personnalisées. Ce paramètre s'applique à toutes les ACL Web pour les ressources que vous gérez dans cette session d'assistant.

Grâce à l'atténuation automatique des attaques DDoS au niveau de la couche applicative, Shield Advanced maintient une règle basée sur le taux dans l'ACL AWS WAF Web de la ressource qui limite le volume de demandes provenant de sources DDoS connues. En outre, Shield Advanced compare les modèles de trafic actuels aux données de référence du trafic historiques afin de détecter les écarts susceptibles d'indiquer une attaque DDoS. Lorsque Shield Advanced détecte une attaque DDoS, il répond en créant, en évaluant et en déployant des AWS WAF règles personnalisées pour y répondre. Vous spécifiez si les règles personnalisées comptent ou bloquent les attaques en votre nom.

> **Note**
>
> L'atténuation automatique des attaques DDoS au niveau de la couche application fonctionne uniquement avec les ACL Web créées à l'aide de la dernière version de AWS WAF (v2).

Pour plus d'informations sur l'atténuation automatique des attaques DDoS par Shield Advanced au niveau de la couche d'application, y compris les mises en garde et les meilleures pratiques relatives à l'utilisation de cette fonctionnalité, consultez. Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative

3. Choisissez Suivant. L'assistant de console passe à la page de détection basée sur l'état de santé.

Configurez la détection basée sur l'état de santé pour vos protections

Configurez Shield Advanced pour utiliser la détection basée sur l'état de santé afin d'améliorer la réactivité et la précision de la détection et de l'atténuation des attaques. Des bilans de santé bien configurés sont essentiels pour une détection précise des événements. Vous pouvez configurer la détection basée sur l'état de santé pour tous les types de ressources, à l'exception des zones hébergées Route 53.

Pour utiliser la détection basée sur l'état de santé, définissez un bilan de santé pour votre ressource dans Route 53, puis associez le bilan de santé à votre protection Shield Advanced. Il est important que le bilan de santé que vous configurez reflète précisément l'état de santé de la ressource. Pour obtenir des informations et des exemples de configuration des contrôles de santé à utiliser avec Shield Advanced, consultezDétection basée sur l'état de santé au moyen de bilans.

Des bilans de santé sont requis pour le support d'engagement proactif de la Shield Response Team (SRT). Pour plus d'informations sur l'engagement proactif, consultezConfiguration de l'engagement proactif.

> **Note**
>
> Les bilans de santé doivent indiquer qu'ils sont sains lorsque vous les associez à vos protections Shield Advanced.

Pour configurer la détection basée sur l'état

1. Sous Associated Health Check (Vérification de l’état de santé associée), choisissez l'ID de la vérification de l’état de santé que vous souhaitez associer à la protection.

   > **Note**
   >
   > Si le bilan de santé dont vous avez besoin ne s'affiche pas, accédez à la console Route 53 et vérifiez le bilan de santé et son identifiant. Pour plus d'informations, consultez Creating and Updating Health Checks (Création et mise à jour des vérifications de l’état de santé).

2. Choisissez Suivant. L'assistant de console passe à la page des alarmes et des notifications.

Configuration des alarmes et des notifications

Vous pouvez éventuellement configurer les notifications Amazon Simple Notification Service pour les CloudWatch alarmes Amazon détectées et l'activité des règles basée sur les taux. Vous pouvez les utiliser pour recevoir une notification lorsque Shield détecte un événement sur une ressource protégée ou lorsqu'une limite de débit configurée dans une règle basée sur le taux est dépassée.

Pour plus d'informations sur CloudWatch les métriques Shield Advanced, consultezAWS Shield Advanced métriques. Pour plus d'informations sur Amazon SNS, consultez le guide du développeur Amazon Simple Notification Service.

Pour configurer les alarmes et les notifications

1. Sélectionnez les rubriques Amazon SNS pour lesquelles vous souhaitez recevoir une notification. Vous pouvez utiliser une seule rubrique Amazon SNS pour toutes les ressources protégées et les règles basées sur les tarifs, ou vous pouvez choisir différents sujets, adaptés à votre organisation. Par exemple, vous pouvez créer une rubrique SNS pour chaque équipe chargée de répondre aux incidents pour un ensemble spécifique de ressources.
2. Choisissez Suivant. L'assistant de console passe à la page de révision de la protection des ressources.

Vérifiez et finalisez votre configuration de protection

Pour vérifier et configurer vos paramètres

1. Sur la page Vérifier et configurer l'atténuation et la visibilité des attaques DDoS, passez en revue vos paramètres. Pour apporter des modifications, choisissez Modifier dans la zone que vous souhaitez modifier. Cela vous ramène à la page associée dans l'assistant de console. Apportez vos modifications, puis choisissez Suivant dans les pages suivantes jusqu'à ce que vous reveniez à la page Révision et configuration de l'atténuation et de la visibilité des attaques DDoS.
2. Choisissez Terminer la configuration. La page Ressources protégées répertorie les ressources que vous venez de protéger.

Configuration du AWS support SRT

La Shield Response Team (SRT) est composée d'ingénieurs en sécurité spécialisés dans la réponse aux événements DDoS. Vous pouvez éventuellement ajouter des autorisations qui permettent au SRT de gérer les ressources en votre nom lors d'un événement DDoS. En outre, vous pouvez configurer le SRT pour qu'il interagisse de manière proactive avec vous si les bilans de santé de Route 53 associés à vos ressources protégées ne fonctionnent pas correctement lors d'un événement détecté. Ces deux ajouts à vos protections permettent de réagir plus rapidement aux événements DDoS.

> **Note**
>
> Pour utiliser les services de la Shield Response Team (SRT), vous devez être abonné au plan Business Support ou au plan Enterprise Support.

Le SRT peut surveiller les données des AWS WAF demandes et les journaux lors des événements de la couche application afin d'identifier le trafic anormal. Ils peuvent aider à élaborer des AWS WAF règles personnalisées pour atténuer les sources de trafic offensantes. Le cas échéant, le SRT peut formuler des recommandations architecturales pour vous aider à mieux aligner vos ressources sur les AWS recommandations.

Pour plus d'informations sur le SRT, consultezAssistance de la Shield Response Team (SRT).

Pour accorder des autorisations au SRT

1. Sur la page de présentation de la AWS Shield console, sous Configurer le support AWS SRT, choisissez Modifier l'accès SRT. La page d'accès à l'Edit AWS Shield Response Team (SRT) s'ouvre.
2. Pour le réglage de l'accès SRT, sélectionnez l'une des options suivantes :

   - Ne pas autoriser le SRT à accéder à mon compte — Shield supprime toutes les autorisations que vous avez précédemment accordées au SRT pour accéder à votre compte et à vos ressources.
   - Créer un nouveau rôle pour que le SRT accède à mon compte — Shield crée un rôle qui fait confiance au principal du service`drt.shield.amazonaws.com`, qui représente le SRT, et y associe la politique `AWSShieldDRTAccessPolicy` gérée. La politique gérée permet au SRT de passer des AWS Shield Advanced appels d' AWS WAF API en votre nom et d'accéder à vos AWS WAF journaux. Pour plus d'informations sur la stratégie gérée, consultez AWS politique gérée : AWSShieldDRTAccessPolicy.
   - Choisissez un rôle existant pour que le SRT accède à mes comptes. Pour cette option, vous devez modifier la configuration du rôle dans AWS Identity and Access Management (IAM) comme suit :

     - Attachez la stratégie gérée `AWSShieldDRTAccessPolicy` au rôle. Cette politique gérée permet au SRT de passer des AWS Shield Advanced appels d' AWS WAF API en votre nom et d'accéder à vos AWS WAF journaux. Pour plus d'informations sur la stratégie gérée, consultez AWS politique gérée : AWSShieldDRTAccessPolicy. Pour plus d'informations sur

l'attachement de la politique gérée à votre rôle, consultez la section Attacher et détacher des politiques IAM.

- Modifiez le rôle pour approuver l'entité de service `drt.shield.amazonaws.com`. Il s'agit du principal de service qui représente le SRT. Pour de plus amples informations, veuillez consulter Éléments de stratégie IAM JSON : Mandataire.

3. Choisissez Save pour enregistrer les changements.

Pour plus d'informations sur la façon de donner à la SRT l'accès à vos protections et à vos données, consultezConfiguration de l'accès pour la Shield Response Team (SRT).

Pour permettre un engagement proactif de la SRT

1. Sur la page de présentation de la AWS Shield console, sous Engagement proactif et contacts, dans la zone des contacts, choisissez Modifier.

   Sur la page Modifier les contacts, fournissez les coordonnées des personnes que vous souhaitez que le SRT contacte pour un engagement proactif.

   Si vous indiquez plusieurs contacts, dans les notes, indiquez les circonstances dans lesquelles chaque contact doit être utilisé. Incluez les désignations des contacts principaux et secondaires, et indiquez les heures de disponibilité et les fuseaux horaires de chaque contact.

   Exemples de notes de contact :

   - Il s'agit d'une hotline ouverte 24 heures sur 24, 7 jours sur 7, 365 jours par an. Travaillez avec l'analyste qui répond et il désignera la personne appropriée pour l'appel.
   - Merci de me contacter si la hotline ne répond pas dans les 5 minutes.

2. Choisissez Enregistrer.

   La page d'aperçu reflète les informations de contact mises à jour.

3. Choisissez Modifier la fonctionnalité d'engagement proactif, sélectionnez Activer, puis sélectionnez Enregistrer pour activer l'engagement proactif.

Pour plus d'informations sur l'engagement proactif, consultezConfiguration de l'engagement proactif.

Créez un tableau de bord DDoS dans CloudWatch et définissez des alarmes CloudWatch

Vous pouvez surveiller les activités DDoS potentielles à l'aide d'Amazon CloudWatch, qui collecte des données brutes auprès de Shield Advanced et les traite en indicateurs lisibles en temps quasi réel. Vous pouvez utiliser les statistiques CloudWatch pour avoir une idée des performances de votre application ou service Web. Pour plus d'informations sur l'utilisation CloudWatch, consultez CloudWatch le guide de CloudWatch l'utilisateur Amazon.

- Pour obtenir des instructions sur la création d'un CloudWatch tableau de bord, consultezSurveillance avec Amazon CloudWatch.
- Pour une description des métriques Shield Advanced que vous pouvez ajouter à votre tableau de bord, consultezAWS Shield Advanced métriques.

Shield Advanced communique des indicateurs de ressources CloudWatch plus fréquemment lors d'événements DDoS que lorsqu'aucun événement n'est en cours. Shield Advanced fournit des statistiques une fois par minute pendant un événement, puis une fois juste après la fin de l'événement. Tant qu'aucun événement n'est en cours, Shield Advanced fournit des statistiques une fois par jour, à l'heure assignée à la ressource. Ce rapport périodique maintient les métriques actives et disponibles pour une utilisation dans vos CloudWatch alarmes personnalisées.

Ceci complète le didacticiel pour démarrer avec Shield Advanced. Pour profiter pleinement des protections que vous avez choisies, continuez à explorer les fonctionnalités et options de Shield Advanced. Pour commencer, familiarisez-vous avec les options qui s'offrent à vous pour consulter les événements Visibilité sur les événements DDoS et y répondreRéagir aux événements DDoS.

Assistance de la Shield Response Team (SRT)

La Shield Response Team (SRT) fournit une assistance supplémentaire aux clients de Shield Advanced. Les SRT sont des ingénieurs en sécurité spécialisés dans la réponse aux événements DDoS. Pour apporter un soutien supplémentaire à votre AWS Support plan, vous pouvez travailler directement avec le SRT, en tirant parti de son expertise dans le cadre de votre flux de travail de réponse aux événements. Pour plus d'informations sur les options et pour obtenir des conseils de configuration, consultez les rubriques suivantes.

> **Note**
>
> Pour utiliser les services de la Shield Response Team (SRT), vous devez être abonné au plan Business Support ou au plan Enterprise Support.

Activités de soutien à la SRT

L'objectif principal d'un engagement avec le SRT est de protéger la disponibilité et les performances de votre application. Selon le type d'événement DDoS et l'architecture de votre application, le SRT peut effectuer une ou plusieurs des actions suivantes :

- AWS WAF analyse des journaux et règles : pour les ressources qui utilisent une ACL AWS WAF Web, le SRT peut analyser vos AWS WAF journaux afin d'identifier les caractéristiques des attaques dans les requêtes Web de votre application. Avec votre approbation lors de l'engagement, le SRT peut apporter des modifications à votre ACL Web afin de bloquer les attaques qu'il a identifiées.
- Créez des mesures d'atténuation personnalisées pour le réseau — Le SRT peut rédiger des mesures d'atténuation personnalisées pour vous en cas d'attaques contre la couche d'infrastructure. Le SRT peut travailler avec vous pour comprendre le trafic attendu pour votre application, pour bloquer le trafic inattendu et pour optimiser les limites de débit de paquets par seconde. Pour plus d'informations, consultez Configuration de mesures d'atténuation personnalisées avec la Shield Response Team (SRT).
- Ingénierie du trafic réseau — Le SRT travaille en étroite collaboration avec les équipes AWS réseau pour protéger les clients de Shield Advanced. Le cas échéant, AWS vous pouvez modifier la façon dont le trafic Internet arrive sur le AWS réseau afin d'allouer une plus grande capacité d'atténuation à votre application.
- Recommandations architecturales — Le SRT peut déterminer que la meilleure façon d'atténuer une attaque nécessite des modifications architecturales afin de mieux s'aligner sur les AWS meilleures pratiques, et il vous aidera à mettre en œuvre ces pratiques. Pour plus d'informations, consultez la section AWS Meilleures pratiques en matière de résilience DDoS.

Rubriques

- Configuration de mesures d'atténuation personnalisées avec la Shield Response Team (SRT)

Configuration de l'accès pour la Shield Response Team (SRT)

Vous pouvez autoriser la Shield Response Team (SRT) à agir en votre nom, en accédant à vos AWS WAF journaux et en appelant les AWS WAF API AWS Shield Advanced et pour gérer les protections. Lors d'événements DDoS liés à la couche applicative, le SRT peut surveiller les AWS WAF demandes afin d'identifier le trafic anormal et d'aider à élaborer des AWS WAF règles personnalisées pour atténuer les sources de trafic indésirables.

En outre, vous pouvez accorder à la SRT l'accès à d'autres données que vous avez stockées dans des compartiments Amazon S3, telles que des captures de paquets ou des journaux provenant d'un Application Load Balancer, d' CloudFrontAmazon ou de sources tierces.

> **Note**
>
> Pour utiliser les services de la Shield Response Team (SRT), vous devez être abonné au plan Business Support ou au plan Enterprise Support.

Pour gérer les autorisations pour le SRT

1. Sur la page de présentation de la AWS Shield console, sous Configurer le support AWS SRT, choisissez Modifier l'accès SRT. La page d'accès à l'Edit AWS Shield Response Team (SRT) s'ouvre.
2. Pour le réglage de l'accès SRT, sélectionnez l'une des options suivantes :
   - Ne pas autoriser le SRT à accéder à mon compte — Shield supprime toutes les autorisations que vous avez précédemment accordées au SRT pour accéder à votre compte et à vos ressources.
   - Créer un nouveau rôle pour que le SRT accède à mon compte — Shield crée un rôle qui fait confiance au principal du service`drt.shield.amazonaws.com`, qui représente le SRT, et y associe la politique `AWSShieldDRTAccessPolicy` gérée. La politique gérée permet au SRT de passer des AWS Shield Advanced appels d' AWS WAF API en votre nom et d'accéder à vos AWS WAF journaux. Pour plus d'informations sur la stratégie gérée, consultez AWS politique gérée : AWSShieldDRTAccessPolicy.

- Choisissez un rôle existant pour que le SRT accède à mes comptes. Pour cette option, vous devez modifier la configuration du rôle dans AWS Identity and Access Management (IAM) comme suit :
  - Attachez la stratégie gérée `AWSShieldDRTAccessPolicy` au rôle. Cette politique gérée permet au SRT de passer des AWS Shield Advanced appels d' AWS WAF API en votre nom et d'accéder à vos AWS WAF journaux. Pour plus d'informations sur la stratégie gérée, consultez AWS politique gérée : AWSShieldDRTAccessPolicy. Pour plus d'informations sur l'attachement de la politique gérée à votre rôle, consultez la section Attacher et détacher des politiques IAM.
  - Modifiez le rôle pour approuver l'entité de service `drt.shield.amazonaws.com`. Il s'agit du principal de service qui représente le SRT. Pour de plus amples informations, veuillez consulter Éléments de stratégie IAM JSON : Mandataire.

3. Pour (facultatif) : accordez l'accès SRT à un compartiment Amazon S3. Si vous devez partager des données qui ne figurent pas dans vos journaux ACL AWS WAF Web, configurez-le. Par exemple, les journaux d'accès à Application Load Balancer, les CloudFront journaux Amazon ou les journaux provenant de sources tierces.

   > **Note**
   >
   > Vous n'avez pas besoin de le faire pour vos journaux ACL AWS WAF Web. Le SRT y accède lorsque vous autorisez l'accès à votre compte.

   a. Configurez les compartiments Amazon S3 conformément aux directives suivantes :

      - Les emplacements des compartiments doivent être identiques Compte AWS à ceux auxquels vous avez accordé l'accès général à la SRT, lors de l'étape précédente, à l'accès à la AWS Shield Response Team (SRT).
      - Les compartiments peuvent être chiffrés en texte brut ou par SSE-S3. Pour plus d'informations sur le chiffrement Amazon S3 SSE-S3, consultez la section Protection des données à l'aide du chiffrement côté serveur avec des clés de chiffrement gérées par Amazon S3 (SSE-S3) dans le guide de l'utilisateur Amazon S3.

        Le SRT ne peut pas afficher ni traiter les journaux stockés dans des compartiments chiffrés avec des clés stockées dans AWS Key Management Service ()AWS KMS.

b. Dans le Shield Advanced (facultatif) : accordez à SRT l'accès à une section de compartiment Amazon S3. Pour chaque compartiment Amazon S3 dans lequel vos données ou vos journaux sont stockés, entrez le nom du compartiment et choisissez Add Bucket. Vous pouvez ajouter jusqu'à 10 compartiments.

   Cela accorde au SRT les autorisations suivantes sur chaque compartiment :`s3:GetBucketLocation`,`s3:GetObject`, et`s3:ListBucket`.

   Si vous souhaitez autoriser le SRT à accéder à plus de 10 compartiments, vous pouvez le faire en modifiant les politiques de compartiment supplémentaires et en accordant manuellement les autorisations répertoriées ici pour le SRT.

   Vous trouverez ci-dessous un exemple de liste de politiques.

```
{
    "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. Choisissez Save pour enregistrer les changements.

Vous pouvez également autoriser le SRT via l'API en créant un rôle IAM, en y attachant la politique AWSShieldDRTAccessPolicy , puis en transmettant le rôle à l'opération AssociatedRTrole.

Configuration de l'engagement proactif

Grâce à un engagement proactif, la Shield Response Team (SRT) vous contacte directement lorsque la disponibilité ou les performances de votre application sont affectées par une éventuelle attaque.

Nous recommandons ce modèle d'engagement car il fournit la réponse SRT la plus rapide et permet au SRT de commencer le dépannage avant même d'avoir établi un contact avec vous.

Un engagement proactif est disponible pour les événements liés à la couche réseau et à la couche transport sur les adresses IP élastiques et les accélérateurs AWS Global Accelerator standard, ainsi qu'en cas d'afflux de requêtes Web sur les CloudFront distributions Amazon et les équilibreurs de charge d'application. L'engagement proactif n'est disponible que pour les protections des ressources Shield Advanced associées à un bilan de santé Amazon Route 53. Pour plus d'informations sur la gestion et l'utilisation des bilans de santé, consultezDétection basée sur l'état de santé au moyen de bilans.

Lors d'un événement détecté par Shield Advanced, le SRT utilise l'état de vos bilans de santé pour déterminer si l'événement est éligible à un engagement proactif. Si tel est le cas, le SRT vous contactera conformément aux instructions de contact que vous fournissez dans votre configuration d'engagement proactif.

Vous pouvez configurer jusqu'à dix contacts pour un engagement proactif, et vous pouvez fournir des notes pour aider le SRT à vous contacter. Vos contacts proactifs doivent être disponibles pour communiquer avec le SRT lors d'événements. Si vous ne disposez pas d'un centre des opérations ouvert 24 heures sur 24, 7 jours sur 7, vous pouvez fournir un téléavertisseur et indiquer cette préférence de contact dans vos notes de contact.

L'engagement proactif exige que vous preniez les mesures suivantes :

- Vous devez être abonné au plan Business Support ou au plan Enterprise Support.
- Vous devez associer un bilan de santé d'Amazon Route 53 à toute ressource que vous souhaitez protéger grâce à un engagement proactif. Le SRT utilise l'état de vos bilans de santé pour déterminer si un événement nécessite un engagement proactif. Il est donc important que vos bilans de santé reflètent avec précision l'état de vos ressources protégées. Pour plus d'informations et de conseils, consultezDétection basée sur l'état de santé au moyen de bilans.
- Pour une ressource associée à une ACL AWS WAF Web, vous devez créer l'ACL Web à l'aide de AWS WAF (v2), qui est la dernière version de AWS WAF.
- Vous devez fournir au moins un contact que le SRT utilisera pour un engagement proactif lors d'un événement. Veillez à ce que vos informations de contact soient complètes et à jour.

Pour permettre un engagement proactif de la SRT

1. Sur la page de présentation de la AWS Shield console, sous Engagement proactif et contacts, dans la zone des contacts, choisissez Modifier.

   Sur la page Modifier les contacts, fournissez les coordonnées des personnes que vous souhaitez que le SRT contacte pour un engagement proactif.

   Si vous indiquez plusieurs contacts, dans les notes, indiquez les circonstances dans lesquelles chaque contact doit être utilisé. Incluez les désignations des contacts principaux et secondaires, et indiquez les heures de disponibilité et les fuseaux horaires de chaque contact.

   Exemples de notes de contact :

   - Il s'agit d'une hotline ouverte 24 heures sur 24, 7 jours sur 7, 365 jours par an. Travaillez avec l'analyste qui répond et il désignera la personne appropriée pour l'appel.
   - Merci de me contacter si la hotline ne répond pas dans les 5 minutes.
2. Choisissez Enregistrer.

   La page d'aperçu reflète les informations de contact mises à jour.
3. Choisissez Modifier la fonctionnalité d'engagement proactif, sélectionnez Activer, puis sélectionnez Enregistrer pour activer l'engagement proactif.

Contacter l'équipe Shield Response (SRT)

Vous pouvez contacter la Shield Response Team (SRT) de l'une des manières suivantes :

Cas de support

Vous pouvez ouvrir un dossier AWS Shielddans la console du AWS Support Center.

Pour obtenir des conseils sur la création d'un dossier de support, consultez le AWS Support Centre.

Sélectionnez la gravité adaptée à votre situation et fournissez vos coordonnées. Dans la description, veuillez fournir le plus de détails possible. Fournissez des informations sur les ressources protégées qui, selon vous, pourraient être affectées, ainsi que sur l'état actuel de votre expérience utilisateur final. Par exemple, si votre expérience utilisateur est dégradée ou que certaines parties de votre application ne sont pas disponibles, fournissez ces informations.

- Pour les attaques DDoS présumées : si la disponibilité ou les performances de votre application sont actuellement affectées par une éventuelle attaque DDoS, choisissez les options de gravité et de contact suivantes :
  - Pour ce qui est du niveau de sévérité, choisissez le niveau de sévérité le plus élevé disponible pour votre plan de support :
    - Pour le support aux entreprises, il s'agit d'une panne du système de production : < 1 heure.
    - Pour le support aux entreprises, il s'agit d'une panne du système critique : < 15 minutes.
  - Pour l'option de contact, sélectionnez Téléphone ou Chat et fournissez vos coordonnées. L'utilisation d'une méthode de contact en direct fournit la réponse la plus rapide.

Engagement proactif

Grâce à un engagement AWS Shield Advanced proactif, le SRT vous contacte directement si le bilan de santé d'Amazon Route 53 associé à votre ressource protégée ne fonctionne pas correctement lors d'un événement détecté. Pour plus d’informations sur cette option, consultez Configuration de l'engagement proactif.

Configuration de mesures d'atténuation personnalisées avec la Shield Response Team (SRT)

Pour vos adresses IP élastiques (EIP) et vos accélérateurs AWS Global Accelerator standard, vous pouvez travailler avec la Shield Response Team (SRT) pour configurer des mesures d'atténuation personnalisées. Cela est utile si vous connaissez une logique spécifique qui doit être appliquée lors de la mise en place d'une mesure d'atténuation. Par exemple, vous souhaiterez peut-être n'autoriser que le trafic provenant de certains pays, appliquer des limites de débit spécifiques, configurer des validations facultatives, interdire des fragments ou n'autoriser que le trafic correspondant à un modèle spécifique de charge utile des paquets.

Voici des exemples de mesures d'atténuation personnalisées courantes :

- Correspondance de modèles : si vous exploitez un service qui interagit avec des applications côté client, vous pouvez choisir de faire correspondre des modèles connus propres à ces applications. Par exemple, vous pouvez exploiter un service de jeu ou de communication qui oblige l'utilisateur final à installer un logiciel spécifique que vous distribuez. Vous pouvez inclure un chiffre magique dans chaque paquet envoyé par l'application à votre service. Vous pouvez faire correspondre jusqu'à 128 octets (séparés ou contigus) d'une charge utile et d'en-têtes de paquets TCP ou UDP non fragmentés. La correspondance peut être exprimée en notation hexadécimale sous la forme

d'un décalage spécifique par rapport au début de la charge utile du paquet ou d'un décalage dynamique suivant une valeur connue. Par exemple, l'atténuation peut rechercher l'octet, `0x01` puis `0x12345678` s'attendre aux quatre octets suivants.

- Spécifique au DNS : si vous gérez votre propre service DNS faisant autorité à l'aide de services tels que Global Accelerator ou Amazon Elastic Compute Cloud (Amazon EC2), vous pouvez demander une atténuation personnalisée qui valide les paquets afin de garantir la validité des requêtes DNS et d'appliquer un score de suspicion qui évalue les attributs spécifiques au trafic DNS.

Pour en savoir plus sur l'utilisation de SRT pour créer des mesures d'atténuation personnalisées, créez un dossier d'assistance sous. AWS Shield Pour en savoir plus sur la création de AWS Support dossiers, consultez Getting started with AWS Support.

Protection des ressources dans AWS Shield Advanced

Vous pouvez ajouter et configurer AWS Shield Advanced des protections pour vos ressources. Vous pouvez gérer les protections pour une seule ressource et vous pouvez regrouper vos ressources protégées dans des collections logiques pour une meilleure gestion des événements. Vous pouvez également suivre les modifications apportées à vos protections Shield Advanced à l'aide de AWS Config.

Rubriques

AWS Shield Advanced protections par type de ressource

Shield Advanced protège les AWS ressources des couches réseau et transport (couches 3 et 4) et de la couche application (couche 7). Vous pouvez protéger certaines ressources directement et d'autres en les associant à des ressources protégées. Shield Advanced prend en charge le protocole IPv4, mais pas le protocole IPv6.

Cette section fournit des informations sur les protections Shield Advanced pour chaque type de ressource.

> **Note**
>
> Shield Advanced protège uniquement les ressources que vous avez spécifiées soit dans Shield Advanced, soit par le biais d'une politique AWS Firewall Manager Shield Advanced. Il ne protège pas automatiquement vos ressources.

Vous pouvez utiliser Shield Advanced pour une surveillance et une protection avancées avec les types de ressources suivants :

- CloudFront Distributions Amazon. Pour CloudFront un déploiement continu, Shield Advanced protège toute distribution intermédiaire associée à une distribution principale protégée.
- Zones hébergées Amazon Route 53.
- AWS Global Accelerator accélérateurs standard.
- Adresses IP élastiques Amazon EC2. Shield Advanced protège les ressources associées aux adresses IP Elastic protégées.
- Instances Amazon EC2, par association à des adresses IP Amazon EC2 Elastic.
- Les équilibreurs de charge Elastic Load Balancing (ELB) suivants :
  - Équilibreurs de charge des applications.
  - Équilibreurs Classic Load Balancer.
  - Équilibreurs de charge réseau, via des associations aux adresses IP Amazon EC2 Elastic.

Vous ne pouvez pas utiliser Shield Advanced pour protéger un autre type de ressource. Par exemple, vous ne pouvez pas protéger les accélérateurs de routage AWS Global Accelerator personnalisés ou les équilibreurs de charge de passerelle.

Vous pouvez surveiller et protéger jusqu'à 1 000 ressources pour chaque type de ressource Compte AWS. Par exemple, dans un seul compte, vous pouvez protéger 1 000 adresses IP Amazon EC2 Elastic, 1 000 CloudFront distributions et 1 000 équilibreurs de charge d'application. Vous pouvez demander une augmentation du nombre de ressources que vous pouvez protéger avec Shield Advanced via la console Service Quotas à l'adresse https://console.aws.amazon.com/servicequotas/.

Protection des instances Amazon EC2 et des équilibreurs de charge réseau avec Shield Advanced

Vous pouvez protéger les instances Amazon EC2 et les Network Load Balancers en associant d'abord ces ressources aux adresses IP Elastic, puis en protégeant les adresses IP Elastic dans Shield Advanced.

Lorsque vous protégez les adresses IP Elastic, Shield Advanced identifie et protège les ressources auxquelles elles sont associées. Shield Advanced identifie automatiquement le type de ressource associée à une adresse IP élastique et applique les détections et mesures d'atténuation appropriées pour cette ressource. Cela inclut la configuration des ACL réseau spécifiques à l'adresse IP élastique. Pour plus d'informations sur l'utilisation des adresses IP élastiques avec vos AWS ressources, consultez les guides suivants : documentation Amazon Elastic Compute Cloud ou documentation Elastic Load Balancing.

Lors d'une attaque, Shield Advanced déploie automatiquement les ACL de votre réseau jusqu'à la limite du AWS réseau. Lorsque les ACL de votre réseau se situent à la limite du réseau, Shield Advanced peut fournir une protection contre les événements DDoS plus importants. Généralement, les ACL réseau sont appliquées à proximité de vos instances Amazon EC2 au sein de votre Amazon VPC. L'ACL réseau ne peut atténuer les attaques que dans la mesure où votre VPC Amazon et votre instance peuvent les gérer. Par exemple, si l'interface réseau attachée à votre instance Amazon EC2 peut traiter jusqu'à 10 Gbit/s, les volumes supérieurs à 10 Gbit/s ralentiront et bloqueront éventuellement le trafic vers cette instance. Lors d'une attaque, Shield Advanced promeut l'ACL de votre réseau jusqu'à la AWS frontière, qui peut traiter plusieurs téraoctets de trafic. Votre ACL réseau est capable de fournir une protection pour votre ressource bien au-delà de la capacité typique de votre réseau. Pour plus d'informations sur les listes ACL réseau, consultez Listes ACL réseau.

Certains outils de dimensionnement, tels que AWS Elastic Beanstalk, ne vous permettent pas d'associer automatiquement une adresse IP élastique à un Network Load Balancer. Dans ces cas, vous devez associer manuellement l'adresse IP élastique.

AWS Shield Advanced protections de la couche d'application (couche 7)

Pour protéger les ressources de la couche application avec Shield Advanced, vous devez commencer par associer une ACL AWS WAF Web à la ressource et y ajouter une ou plusieurs règles basées sur le débit. Vous pouvez également activer l'atténuation automatique des attaques DDoS au niveau de la couche application, ce qui permet à Shield Advanced de créer et de gérer automatiquement des règles ACL Web en votre nom en réponse aux attaques DDoS.

Lorsque vous protégez une ressource de la couche d'application avec Shield Advanced, Shield Advanced analyse le trafic au fil du temps afin d'établir et de maintenir des bases de référence. Shield Advanced utilise ces bases de référence pour détecter les anomalies dans les modèles de trafic susceptibles d'indiquer une attaque DDoS. Le moment où Shield Advanced détecte une attaque dépend du trafic que Shield Advanced a pu observer avant l'attaque et de l'architecture que vous utilisez pour vos applications Web. Les variations architecturales qui peuvent affecter le comportement de Shield Advanced incluent le type d'instance que vous utilisez, la taille de votre instance et si le type d'instance prend en charge la mise en réseau améliorée. Vous pouvez également configurer Shield Advanced pour mettre automatiquement en place des mesures d'atténuation en cas d'attaques contre la couche application.

Abonnements et AWS WAF coûts de Shield Advanced

Votre abonnement Shield Advanced couvre les coûts liés à l'utilisation des AWS WAF fonctionnalités standard pour les ressources que vous protégez avec Shield Advanced. Les AWS WAF frais standard couverts par vos protections Shield Advanced sont le coût par ACL Web, le coût par règle et le prix de base par million de demandes d'inspection de requêtes Web, jusqu'à 1 500 WCU et jusqu'à la taille corporelle par défaut.

L'activation de l'atténuation automatique des attaques DDoS par la couche application Shield Advanced ajoute un groupe de règles à votre ACL Web qui utilise 150 unités de capacité ACL Web (WCU). Ces WCU sont pris en compte dans l'utilisation des WCU dans votre ACL Web. Pour plus d’informations, consultez Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative, Le groupe de règles Shield Advanced et AWS WAF unités de capacité ACL Web (WCU).

Votre abonnement à Shield Advanced ne couvre pas l'utilisation de AWS WAF ressources que vous ne protégez pas à l'aide de Shield Advanced. Il ne couvre pas non plus les AWS WAF coûts non standard supplémentaires liés aux ressources protégées. Des exemples de AWS WAF coûts non standard sont ceux liés au contrôle des robots, à l'action des CAPTCHA règles, aux ACL Web qui utilisent plus de 1 500 WCU et à l'inspection du corps de la demande au-delà de la taille par défaut. La liste complète est disponible sur la page de AWS WAF tarification.

Pour obtenir des informations complètes et des exemples de tarification, consultez Shield Pricing and AWS WAF Pricing.

Rubriques

- Détection et atténuation
- Shield Advanced, couche d'application, ACL AWS WAF Web et règles basées sur le débit

- Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative

Détection et atténuation

Cette section décrit les facteurs qui affectent la détection et l'atténuation des événements de la couche application par Shield Advanced.

Surveillance de l'état

Les bilans de santé qui indiquent avec précision l'état général de votre application fournissent à Shield Advanced des informations sur les conditions de trafic rencontrées par votre application. Shield Advanced nécessite moins d'informations indiquant une attaque potentielle lorsque votre application signale un dysfonctionnement et davantage de preuves d'une attaque si votre application indique qu'elle est saine.

Il est important de configurer vos bilans de santé de manière à ce qu'ils indiquent avec précision l'état de santé des applications. Pour plus d'informations et de conseils, consultezDétection basée sur l'état de santé au moyen de bilans.

Lignes de référence relatives au trafic

Les lignes de base de trafic fournissent à Shield Advanced des informations sur les caractéristiques du trafic normal pour votre application. Shield Advanced utilise ces lignes de base pour identifier les cas où votre application ne reçoit pas de trafic normal. Il peut ainsi vous avertir et, une fois configuré, commencer à concevoir et à tester des options d'atténuation pour contrer une attaque potentielle. Pour plus d'informations sur la manière dont Shield Advanced utilise les bases de trafic pour détecter les événements potentiels, consultez la section Logique de détection des menaces pesant sur la couche applicative de présentation.

Shield Advanced crée ses lignes de base à partir des informations fournies par l'ACL Web associée à la ressource protégée. L'ACL Web doit être associée à la ressource pendant au moins 24 heures et jusqu'à 30 jours avant que Shield Advanced puisse déterminer de manière fiable les bases de référence de l'application. Le temps requis commence lorsque vous associez l'ACL Web, soit via Shield Advanced, soit via AWS WAF.

Pour plus d'informations sur l'utilisation d'une ACL Web avec les protections de la couche d'application Shield Advanced, consultezShield Advanced, couche d'application, ACL AWS WAF Web et règles basées sur le débit.

Règles basées sur un débit

Les règles basées sur le taux peuvent aider à atténuer les attaques. Ils peuvent également masquer les attaques, en les atténuant avant qu'elles ne deviennent un problème suffisamment important pour apparaître par rapport aux données de référence normales en matière de trafic ou dans les rapports d'état des bilans de santé.

Nous vous recommandons d'utiliser des règles basées sur le taux dans votre ACL Web lorsque vous protégez une ressource d'application avec Shield Advanced. Même si leurs mesures d'atténuation peuvent masquer une attaque potentielle, elles constituent une première ligne de défense précieuse, car elles permettent de garantir que votre application reste accessible à vos clients légitimes. Le trafic détecté par vos règles basées sur les taux et les limites de débit est visible dans vos AWS WAF statistiques.

Outre vos propres règles basées sur le taux, si vous activez l'atténuation automatique des attaques DDoS au niveau de la couche application, Shield Advanced ajoute un groupe de règles à votre ACL Web qu'il utilise pour atténuer les attaques. Dans ce groupe de règles, Shield Advanced dispose toujours d'une règle basée sur le débit qui limite le volume de demandes provenant d'adresses IP connues pour être à l'origine d'attaques DDoS. Vous ne pouvez pas consulter les statistiques du trafic que les règles Shield Advanced atténuent.

Pour plus d'informations sur les règles basées sur les taux, consultezInstruction de règle basée sur un taux. Pour plus d'informations sur la règle basée sur le débit utilisée par Shield Advanced pour l'atténuation automatique des attaques DDoS au niveau de la couche application, consultez. Le groupe de règles Shield Advanced

Pour plus d'informations sur Shield Advanced et AWS WAF les métriques, consultezSurveillance avec Amazon CloudWatch.

Shield Advanced, couche d'application, ACL AWS WAF Web et règles basées sur le débit

Pour protéger une ressource de la couche application avec Shield Advanced, vous devez commencer par associer une ACL AWS WAF Web à la ressource. AWS WAF est un pare-feu d'applications Web qui vous permet de surveiller les requêtes HTTP et HTTPS qui sont transmises aux ressources de la couche application et de contrôler l'accès à votre contenu en fonction des caractéristiques des demandes. Vous pouvez configurer une ACL Web pour surveiller et gérer les demandes en fonction de facteurs tels que l'origine de la demande, le contenu des chaînes de requête et des cookies, et le taux de demandes provenant d'une seule adresse IP. Au minimum, votre protection Shield Advanced vous oblige à associer une ACL Web à une règle basée sur le débit, qui limite le taux de demandes pour chaque adresse IP.

Si aucune règle basée sur le taux n'est définie dans l'ACL Web associée, Shield Advanced vous invite à en définir au moins une. Les règles basées sur le débit bloquent automatiquement le trafic provenant des adresses IP sources lorsqu'elles dépassent les seuils que vous définissez. Ils aident à protéger votre application contre les inondations de requêtes Web et peuvent fournir des alertes en cas de pics de trafic soudains susceptibles d'indiquer une attaque DDoS potentielle.

> **Note**
>
> Une règle basée sur le taux répond très rapidement aux pics de trafic surveillés par la règle. De ce fait, une règle basée sur le taux peut empêcher non seulement une attaque, mais également la détection d'une attaque potentielle par le biais de la fonction de détection Shield Advanced. Ce compromis privilégie la prévention plutôt que la visibilité complète des modèles d'attaque. Nous vous recommandons d'utiliser une règle basée sur le taux comme première ligne de défense contre les attaques.

Une fois votre ACL Web en place, en cas d'attaque DDoS, vous appliquez des mesures d'atténuation en ajoutant et en gérant des règles dans l'ACL Web. Vous pouvez le faire directement, avec l'aide de la Shield Response Team (SRT), ou automatiquement grâce à l'atténuation automatique des attaques DDoS au niveau de la couche application.

> **Important**
>
> Si vous utilisez également l'atténuation automatique des attaques DDoS au niveau de la couche application, consultez les meilleures pratiques pour gérer votre ACL Web à l'Bonnes pratiques pour l'utilisation de l'atténuation automatiqueadresse.

Comportement des règles basé sur le taux par défaut

Lorsque vous utilisez une règle basée sur le taux avec sa configuration par défaut, elle évalue AWS WAF régulièrement le trafic pour la période de 5 minutes précédente. AWS WAF bloque les demandes provenant de toute adresse IP qui dépasse le seuil de la règle jusqu'à ce que le taux de demandes descende à un niveau acceptable. Lorsque vous configurez une règle basée sur le débit via Shield Advanced, configurez son seuil de débit à une valeur supérieure au débit de trafic normal que vous attendez d'une adresse IP source sur une fenêtre de cinq minutes.

Vous souhaiterez peut-être utiliser plusieurs règles basées sur le taux dans une ACL Web. Par exemple, vous pouvez avoir une règle basée sur le taux pour tout le trafic dont le seuil est élevé, plus

une ou plusieurs règles supplémentaires configurées pour correspondre à certaines parties de votre application Web et dont les seuils sont inférieurs. Par exemple, vous pouvez faire correspondre l'URI `/login.html` avec un seuil inférieur, afin de limiter les abus commis contre une page de connexion.

Vous pouvez configurer une règle basée sur le taux pour utiliser une fenêtre temporelle d'évaluation différente et pour agréger les demandes en fonction d'un certain nombre de composants de demande, tels que les valeurs d'en-tête, les étiquettes et les arguments de requête. Pour plus d'informations, consultez Instruction de règle basée sur un taux.

Pour plus d'informations et de conseils, consultez le billet de blog sur la sécurité Les trois règles AWS WAF basées sur les taux les plus importantes.

Options de configuration étendues grâce à AWS WAF

La console Shield Advanced vous permet d'ajouter une règle basée sur le taux et de la configurer avec les paramètres de base par défaut. Vous pouvez définir des options de configuration supplémentaires en gérant vos règles basées sur les taux via AWS WAF. Par exemple, vous pouvez configurer la règle pour agréger les demandes en fonction de clés telles qu'une adresse IP transférée, une chaîne de requête et une étiquette. Vous pouvez également ajouter une instruction scope-down à la règle afin de soustraire certaines demandes à l'évaluation et à la limitation du débit. Pour plus d'informations, consultez Instruction de règle basée sur un taux. Pour plus d'informations sur l'utilisation AWS WAF des règles de surveillance et de gestion de vos requêtes Web pour gérer, consultezCréation d'une liste ACL web.

Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative

Vous pouvez configurer Shield Advanced pour qu'il réponde automatiquement afin d'atténuer les attaques de la couche application (couche 7) contre les ressources de la couche application protégée, en comptant ou en bloquant les requêtes Web faisant partie de l'attaque. Cette option vient s'ajouter à la protection de la couche application que vous ajoutez via Shield Advanced avec une ACL AWS WAF Web et votre propre règle basée sur le taux.

Lorsque l'atténuation automatique est activée pour une ressource, Shield Advanced gère un groupe de règles dans l'ACL Web associée à la ressource, dans lequel il gère les règles d'atténuation au nom de la ressource. Le groupe de règles contient une règle basée sur le débit qui suit le volume de demandes provenant d'adresses IP connues pour être à l'origine d'attaques DDoS.

En outre, Shield Advanced compare les modèles de trafic actuels aux données de référence du trafic historiques afin de détecter les écarts susceptibles d'indiquer une attaque DDoS. Shield Advanced

répond aux attaques DDoS détectées en créant, en évaluant et en déployant des AWS WAF règles personnalisées supplémentaires dans le groupe de règles.

Table des matières

Mises en garde relatives à l'utilisation de l'atténuation automatique

La liste suivante décrit les inconvénients de l'atténuation automatique des attaques DDoS au niveau de la couche applicative Shield Advanced et décrit les mesures que vous pouvez prendre pour y remédier.

- L'atténuation automatique des attaques DDoS au niveau de la couche application fonctionne uniquement avec les ACL Web créées à l'aide de la dernière version de AWS WAF (v2).
- Shield Advanced a besoin de temps pour établir une base de référence du trafic historique normal de votre application, qu'il utilise pour détecter et isoler le trafic d'attaque du trafic normal, afin

d'atténuer le trafic d'attaque. Le délai d'établissement d'une base de référence est compris entre 24 heures et 30 jours à compter du moment où vous associez une ACL Web à la ressource d'application protégée. Pour plus d'informations sur les lignes de base du trafic, consultezDétection et atténuation.

- L'activation de l'atténuation automatique des attaques DDoS au niveau de la couche application ajoute un groupe de règles à votre ACL Web qui utilise 150 unités de capacité ACL Web (WCU). Ces WCU sont pris en compte dans l'utilisation des WCU dans votre ACL Web. Pour plus d'informations, consultez Le groupe de règles Shield Advanced et AWS WAF unités de capacité ACL Web (WCU).
- Le groupe de règles Shield Advanced génère AWS WAF des métriques, mais elles ne peuvent pas être consultées. Il en va de même pour tous les autres groupes de règles que vous utilisez dans votre ACL Web mais dont vous n'êtes pas propriétaire, tels que les groupes de règles AWS gérées. Pour plus d'informations sur AWS WAF les métriques, consultezAWS WAF métriques et dimensions. Pour plus d'informations sur cette option de protection Shield Advanced, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.
- Pour les ACL Web qui protègent plusieurs ressources, l'atténuation automatique déploie uniquement des mesures d'atténuation personnalisées qui n'ont aucun impact négatif sur les ressources protégées.
- Le délai entre le début d'une attaque DDoS et le moment où Shield Advanced place des règles d'atténuation automatique personnalisées varie en fonction de chaque événement. Certaines attaques DDoS peuvent prendre fin avant que les règles personnalisées ne soient déployées. D'autres attaques peuvent se produire lorsqu'une atténuation est déjà en place et peuvent donc être atténuées par ces règles dès le début de l'événement. En outre, les règles basées sur le taux dans le groupe de règles Web ACL et Shield Advanced peuvent atténuer le trafic d'attaque avant qu'il ne soit détecté comme un événement potentiel.
- Pour les équilibreurs de charge d'application qui reçoivent du trafic via un réseau de diffusion de contenu (CDN), tel qu'Amazon CloudFront, les capacités d'atténuation automatique de la couche applicative de Shield Advanced pour ces ressources d'Application Load Balancer seront réduites. Shield Advanced utilise les attributs du trafic client pour identifier et isoler le trafic d'attaque du trafic normal vers votre application, et les CDN peuvent ne pas conserver ou transmettre les attributs du trafic client d'origine. Si vous l'utilisez CloudFront, nous vous recommandons d'activer l'atténuation automatique sur la CloudFront distribution.
- L'atténuation automatique des attaques DDoS au niveau de la couche applicative n'interagit pas avec les groupes de protection. Vous pouvez activer l'atténuation automatique pour les ressources

appartenant à des groupes de protection, mais Shield Advanced n'applique pas automatiquement les mesures d'atténuation des attaques en fonction des résultats des groupes de protection. Shield Advanced applique des mesures d'atténuation automatiques des attaques pour les ressources individuelles.

Bonnes pratiques pour l'utilisation de l'atténuation automatique

Respectez les instructions fournies dans cette section lorsque vous utilisez l'atténuation automatique.

Gestion générale des protections

Suivez ces directives pour planifier et mettre en œuvre vos protections d'atténuation automatiques.

- Gérez toutes vos protections d'atténuation automatique via Shield Advanced ou, si vous utilisez AWS Firewall Manager pour gérer vos paramètres d'atténuation automatique de Shield Advanced, via Firewall Manager. Ne mélangez pas l'utilisation de Shield Advanced et de Firewall Manager pour gérer ces protections.
- Gérez des ressources similaires à l'aide des mêmes ACL Web et des mêmes paramètres de protection, et gérez des ressources différentes à l'aide de différentes ACL Web. Lorsque Shield Advanced atténue une attaque DDoS sur une ressource protégée, il définit des règles pour l'ACL Web associée à la ressource, puis teste les règles par rapport au trafic de toutes les ressources associées à l'ACL Web. Shield Advanced n'appliquera les règles que si elles n'ont aucun impact négatif sur les ressources associées. Pour plus d’informations, consultez Comment Shield Advanced gère l'atténuation automatique.
- Pour les équilibreurs de charge d'application dont tout le trafic Internet est transmis par proxy via une CloudFront distribution Amazon, activez uniquement l'atténuation automatique sur la distribution. CloudFront La CloudFront distribution comportera toujours le plus grand nombre d'attributs de trafic d'origine, que Shield Advanced exploite pour atténuer les attaques.

Optimisation de la détection et de l'atténuation

Suivez ces directives pour optimiser les protections que l'atténuation automatique fournit aux ressources protégées. Pour une vue d'ensemble de la détection et de l'atténuation de la couche d'application, voirDétection et atténuation.

- Configurez des contrôles de santé pour vos ressources protégées et utilisez-les pour activer la détection basée sur l'état dans vos protections Shield Advanced. Pour de plus amples informations, consultez Détection basée sur l'état de santé au moyen de bilans.

- Activez l'atténuation automatique en Count mode jusqu'à ce que Shield Advanced ait établi une base de référence pour le trafic historique normal. Shield Advanced a besoin de 24 heures à 30 jours pour établir une base de référence.

  L'établissement d'une base de référence des modèles de trafic normaux nécessite les éléments suivants :

  - L'association d'une ACL Web à la ressource protégée. Vous pouvez l'utiliser AWS WAF directement pour associer votre ACL Web ou vous pouvez demander à Shield Advanced de l'associer lorsque vous activez la protection de la couche d'application Shield Advanced et que vous spécifiez une ACL Web à utiliser.
  - Flux de trafic normal vers votre application protégée. Si le trafic de votre application n'est pas normal, par exemple avant son lancement ou si le trafic de production est insuffisant pendant de longues périodes, les données historiques ne peuvent pas être collectées.

Gestion des ACL Web

Suivez ces instructions pour gérer les ACL Web que vous utilisez avec une atténuation automatique.

- Si vous devez remplacer l'ACL Web associée à la ressource protégée, apportez les modifications suivantes dans l'ordre :

  1. Dans Shield Advanced, désactivez l'atténuation automatique.
  2. Dans AWS WAF, dissociez l'ancienne ACL Web et associez la nouvelle ACL Web.
  3. Dans Shield Advanced, activez l'atténuation automatique.

  Shield Advanced ne transfère pas automatiquement l'atténuation automatique de l'ancienne ACL Web vers la nouvelle.
- Ne supprimez aucune règle de groupe de règles de vos ACL Web dont le nom commence `ShieldMitigationRuleGroup` par. Si vous supprimez ce groupe de règles, vous désactivez les protections fournies par l'atténuation automatique de Shield Advanced pour chaque ressource associée à l'ACL Web. En outre, Shield Advanced peut mettre un certain temps à recevoir la notification du changement et à mettre à jour ses paramètres. Pendant ce temps, les pages de la console Shield Advanced fourniront des informations incorrectes.

  Pour plus d'informations sur le groupe de règles, consultezLe groupe de règles Shield Advanced.
- Ne modifiez pas le nom d'une règle de groupe de règles dont le nom commence par`ShieldMitigationRuleGroup`. Cela peut interférer avec les protections fournies par l'atténuation automatique de Shield Advanced via l'ACL Web.

- Lorsque vous créez des règles et des groupes de règles, n'utilisez pas de noms commençant par`ShieldMitigationRuleGroup`. Cette chaîne est utilisée par Shield Advanced pour gérer vos mesures d'atténuation automatiques.
- Dans le cadre de la gestion de vos règles ACL Web, n'attribuez pas de paramètre de priorité de 10 000 000. Shield Advanced attribue ce paramètre de priorité à sa règle de groupe de règles d'atténuation automatique lorsqu'il l'ajoute.
- Priorisez la `ShieldMitigationRuleGroup` règle afin qu'elle s'exécute quand vous le souhaitez par rapport aux autres règles de votre ACL Web. Shield Advanced ajoute la règle du groupe de règles à l'ACL Web avec une priorité de 10 000 000, à exécuter après vos autres règles. Si vous utilisez l'assistant de AWS WAF console pour gérer votre ACL Web, ajustez les paramètres de priorité selon vos besoins après avoir ajouté des règles à l'ACL Web.
- Si vous avez l' AWS CloudFormation habitude de gérer vos ACL Web, vous n'avez pas besoin de gérer la `ShieldMitigationRuleGroup` règle du groupe de règles. Suivez les instructions surUtilisation AWS CloudFormation avec atténuation automatique des attaques DDoS au niveau de la couche applicative.

Configuration requise pour activer l'atténuation automatique

Vous activez l'atténuation automatique de Shield Advanced dans le cadre des protections DDoS de la couche application pour votre ressource. Pour plus d'informations sur cette opération via la console, consultezConfiguration des protections DDoS au niveau de la couche applicative.

La fonctionnalité d'atténuation automatique vous oblige à effectuer les opérations suivantes :

- Associez une ACL Web à la ressource : cela est nécessaire pour toute protection de la couche d'application Shield Advanced. Vous pouvez utiliser la même ACL Web pour plusieurs ressources. Nous vous recommandons de le faire uniquement pour les ressources ayant un trafic similaire. Pour plus d'informations sur les ACL Web, notamment les exigences relatives à leur utilisation avec plusieurs ressources, consultezComment AWS WAF fonctionne.
- Activez et configurez l'atténuation automatique des attaques DDoS au niveau de la couche application de Shield Advanced : lorsque vous activez cette option, vous indiquez si vous souhaitez que Shield Advanced bloque ou compte automatiquement les requêtes Web considérées comme faisant partie d'une attaque DDoS. Shield Advanced ajoute un groupe de règles à l'ACL Web associée et l'utilise pour gérer dynamiquement sa réponse aux attaques DDoS sur la ressource. Pour plus d'informations sur les options d'action des règles, consultezAction de la règle.

- (Facultatif, mais recommandé) Ajoutez une règle basée sur le débit à l'ACL Web — Par défaut, la règle basée sur le débit fournit à votre ressource une protection de base contre les attaques DDoS en empêchant toute adresse IP individuelle d'envoyer trop de demandes en peu de temps. Pour plus d'informations sur les règles basées sur le taux, y compris les options d'agrégation de demandes personnalisées et des exemples, consultezInstruction de règle basée sur un taux.

Comment Shield Advanced gère l'atténuation automatique

Les rubriques de la section décrivent comment Shield Advanced gère vos modifications de configuration pour l'atténuation automatique des attaques DDoS au niveau de la couche application et comment il gère les attaques DDoS lorsque l'atténuation automatique est activée.

Rubriques

- Que se passe-t-il lorsque vous activez l'atténuation automatique
- Comment Shield Advanced répond aux attaques DDoS grâce à une atténuation automatique
- Comment Shield Advanced gère le paramètre d'action des règles
- Comment Shield Advanced gère les mesures d'atténuation lorsqu'une attaque s'atténue
- Que se passe-t-il lorsque vous désactivez l'atténuation automatique

Que se passe-t-il lorsque vous activez l'atténuation automatique

Shield Advanced effectue les opérations suivantes lorsque vous activez l'atténuation automatique :

- Le cas échéant, ajoute un groupe de règles pour une utilisation dans Shield Advanced. Si l'ACL AWS WAF Web que vous avez associée à la ressource ne dispose pas encore d'une AWS WAF règle de groupe de règles dédiée à l'atténuation automatique des attaques DDoS au niveau de la couche application, Shield Advanced en ajoute une.

  Le nom de la règle du groupe de règles commence par`ShieldMitigationRuleGroup`. Le groupe de règles contient toujours une règle basée sur le débit nommée`ShieldKnownOffenderIPRateBasedRule`, qui limite le volume de demandes provenant d'adresses IP connues pour être à l'origine d'attaques DDoS. Pour plus de détails sur le groupe de règles Shield Advanced et la règle ACL Web qui y fait référence, consultezLe groupe de règles Shield Advanced.
- Commence à répondre aux attaques DDoS contre la ressource — Shield Advanced répond automatiquement aux attaques DDoS visant la ressource protégée. Outre la règle basée sur le taux, qui est toujours présente, Shield Advanced utilise son groupe de AWS WAF règles pour

déployer des règles personnalisées visant à atténuer les attaques DDoS. Shield Advanced adapte ces règles à votre application et aux attaques qu'elle subit, et les teste par rapport au trafic historique de la ressource avant de les déployer.

Shield Advanced utilise une règle de groupe de règles unique dans toutes les ACL Web que vous utilisez pour une atténuation automatique. Si Shield Advanced a déjà ajouté le groupe de règles pour une autre ressource protégée, il n'ajoute aucun autre groupe de règles à l'ACL Web.

L'atténuation automatique des attaques DDoS au niveau de la couche applicative dépend de la présence du groupe de règles pour atténuer les attaques. Si le groupe de règles est supprimé de l'ACL AWS WAF Web pour une raison quelconque, la suppression désactive l'atténuation automatique pour toutes les ressources associées à l'ACL Web.

Comment Shield Advanced répond aux attaques DDoS grâce à une atténuation automatique

Lorsque l'atténuation automatique est activée sur une ressource protégée, la règle `ShieldKnownOffenderIPRateBasedRule` basée sur le taux du groupe de règles Shield Advanced répond automatiquement aux volumes de trafic élevés provenant de sources DDoS connues. Cette limitation de débit est appliquée rapidement et constitue une défense de première ligne contre les attaques.

Lorsque Shield Advanced détecte une attaque, il effectue les opérations suivantes :

1. Tente d'identifier une signature d'attaque qui isole le trafic d'attaque du trafic normal vers votre application. L'objectif est de produire des règles d'atténuation des attaques DDoS de haute qualité qui, une fois mises en place, n'affectent que le trafic d'attaque et n'ont aucun impact sur le trafic normal de votre application.
2. Évalue la signature d'attaque identifiée par rapport aux modèles de trafic historiques pour la ressource attaquée ainsi que pour toute autre ressource associée à la même ACL Web. Shield Advanced le fait avant de déployer des règles en réponse à l'événement.

   En fonction des résultats de l'évaluation, Shield Advanced effectue l'une des opérations suivantes :

   - Si Shield Advanced détermine que la signature d'attaque isole uniquement le trafic impliqué dans l'attaque DDoS, il implémente la signature dans les règles du groupe de AWS WAF règles d'atténuation Shield Advanced de l'ACL Web. Shield Advanced attribue à ces règles le paramètre d'action que vous avez configuré pour l'atténuation automatique de la ressource, Count soitBlock.
   - Dans le cas contraire, Shield Advanced ne place aucune mesure d'atténuation.

Tout au long d'une attaque, Shield Advanced envoie les mêmes notifications et fournit les mêmes informations sur les événements que pour les protections de base de la couche d'application Shield Advanced. Vous pouvez consulter les informations sur les événements et les attaques DDoS, ainsi que sur les mesures d'atténuation mises en place par Shield Advanced en cas d'attaques, dans la console d'événements Shield Advanced. Pour plus d'informations, consultez Visibilité sur les événements DDoS.

Si vous avez configuré l'atténuation automatique pour utiliser l'action des Block règles et que les règles d'atténuation déployées par Shield Advanced présentent des faux positifs, vous pouvez modifier l'action de la règle enCount. Pour plus d'informations sur la procédure à suivre, consultezModification de l'action utilisée pour l'atténuation automatique des attaques DDoS au niveau de la couche applicative.

Comment Shield Advanced gère le paramètre d'action des règles

Vous pouvez définir l'action de la règle pour vos mesures d'atténuation automatiques sur Block ouCount.

Lorsque vous modifiez le paramètre d'action de la règle d'atténuation automatique pour une ressource protégée, Shield Advanced met à jour tous les paramètres des règles pour la ressource. Il met à jour toutes les règles actuellement en place pour la ressource du groupe de règles Shield Advanced et utilise le nouveau paramètre d'action lorsqu'il crée de nouvelles règles.

Pour les ressources qui utilisent la même ACL Web, si vous spécifiez des actions différentes, Shield Advanced utilise le paramètre Block d'action de la règle `ShieldKnown0ffenderIPRateBasedRule` basée sur le taux du groupe de règles. Shield Advanced crée et gère les autres règles du groupe de règles pour le compte d'une ressource protégée spécifique, et utilise le paramètre d'action que vous avez spécifié pour la ressource. Toutes les règles du groupe de règles Shield Advanced d'une ACL Web sont appliquées au trafic Web de toutes les ressources associées.

La modification du paramètre d'action peut prendre quelques secondes pour se propager. Pendant ce temps, il est possible que vous voyiez l'ancien paramètre à certains endroits où le groupe de règles est utilisé, et le nouveau paramètre à d'autres endroits.

Vous pouvez modifier le paramètre d'action des règles pour votre configuration d'atténuation automatique sur la page des événements de la console et via la page de configuration de la couche application. Pour plus d'informations sur la page des événements, consultezRéagir aux événements DDoS. Pour plus d'informations sur la page de configuration, consultezConfiguration des protections DDoS au niveau de la couche applicative.

Comment Shield Advanced gère les mesures d'atténuation lorsqu'une attaque s'atténue

Lorsque Shield Advanced détermine que les règles d'atténuation déployées pour une attaque particulière ne sont plus nécessaires, il les supprime du groupe de règles d'atténuation Shield Advanced.

La suppression des règles atténuantes ne coïncidera pas nécessairement avec la fin d'une attaque. Shield Advanced surveille les types d'attaques qu'il détecte sur vos ressources protégées. Il peut se défendre de manière proactive contre la récurrence d'une attaque portant une signature spécifique en maintenant en place les règles qu'il a déployées contre la survenue initiale de cette attaque. Au besoin, Shield Advanced augmente la période pendant laquelle il maintient les règles en place. Shield Advanced peut ainsi atténuer les attaques répétées avec une signature spécifique avant qu'elles n'affectent vos ressources protégées.

Shield Advanced ne supprime jamais la règle basée sur le débit`ShieldKnown0ffenderIPRateBasedRule`, qui limite le volume de demandes provenant d'adresses IP connues pour être à l'origine d'attaques DDoS.

Que se passe-t-il lorsque vous désactivez l'atténuation automatique

Shield Advanced effectue les opérations suivantes lorsque vous désactivez l'atténuation automatique pour une ressource :

- Arrête de répondre automatiquement aux attaques DDoS : Shield Advanced arrête ses activités de réponse automatique pour la ressource.
- Supprime les règles inutiles du groupe de règles Shield Advanced : si Shield Advanced gère des règles dans son groupe de règles géré pour le compte de la ressource protégée, il les supprime.
- Supprime le groupe de règles Shield Advanced s'il n'est plus utilisé : si l'ACL Web que vous avez associée à la ressource n'est associée à aucune autre ressource pour laquelle l'atténuation automatique est activée, Shield Advanced supprime sa règle de groupe de règles de l'ACL Web.

Le groupe de règles Shield Advanced

Shield Advanced gère les activités d'atténuation automatique à l'aide des règles d'un groupe de règles qu'il possède et gère pour vous. Shield Advanced fait référence au groupe de règles par une règle de l'ACL Web que vous avez associée à votre ressource protégée.

La règle du groupe de règles dans votre ACL Web

La règle de groupe de règles Shield Advanced de votre ACL Web possède les propriétés suivantes :

- Nom – `ShieldMitigationRuleGroup_`*`account-id`*`_`*`web-acl-id`*`_`*`unique-identifier`*
- Unités de capacité Web ACL (WCU) — 150. Ces WCU sont pris en compte dans l'utilisation des WCU dans votre ACL Web.

Shield Advanced crée cette règle dans votre ACL Web avec un paramètre de priorité de 10 000 000, afin qu'elle s'exécute après vos autres règles et groupes de règles dans l'ACL Web. AWS WAF exécute les règles dans une ACL Web à partir du paramètre de priorité numérique le plus bas. Au cours de votre gestion de l'ACL Web, ce paramètre de priorité peut changer.

La fonctionnalité d'atténuation automatique ne consomme aucune AWS WAF ressource supplémentaire sur votre compte, à l'exception des WCU utilisées par le groupe de règles dans votre ACL Web. Par exemple, le groupe de règles Shield Advanced n'est pas considéré comme l'un des groupes de règles de votre compte. Pour plus d'informations sur les limites de compte dans AWS WAF, voirAWS WAF quotas.

Règles du groupe de règles

Au sein du groupe de règles Shield Advanced référencé, Shield Advanced applique une règle basée sur le débit`ShieldKnownOffenderIPRateBasedRule`, qui limite le volume de demandes provenant d'adresses IP connues pour être à l'origine d'attaques DDoS. Cette règle constitue la première ligne de défense contre toute attaque, car elle est toujours présente dans le groupe de règles et ne repose pas sur l'analyse des modèles de trafic pour contenir les attaques. L'action de cette règle est définie en fonction de l'action que vous avez choisie pour vos atténuations automatiques, tout comme les autres règles du groupe de règles. Pour plus d'informations sur les règles basées sur les taux, consultezInstruction de règle basée sur un taux.

> **Note**
>
> La règle basée sur le taux `ShieldKnownOffenderIPRateBasedRule` fonctionne indépendamment de la détection d'événements Shield Advanced. Bien que l'atténuation automatique soit activée, cette règle limite le débit des adresses IP connues pour être à l'origine d'attaques DDoS. Pour ces adresses IP, la limitation du débit prévue par la règle permet de prévenir les attaques et d'empêcher les attaques d'apparaître dans les informations de détection du Shield Advanced. Ce compromis privilégie la prévention plutôt que la visibilité complète des modèles d'attaque.

Outre la règle permanente basée sur le taux décrite ci-dessus, le groupe de règles contient toutes les règles que Shield Advanced utilise actuellement pour atténuer les attaques DDoS. Shield Advanced ajoute, modifie et supprime ces règles selon les besoins. Pour plus d'informations, consultez Comment Shield Advanced gère l'atténuation automatique.

Métriques

Le groupe de règles génère AWS WAF des métriques, mais comme ce groupe de règles appartient à Shield Advanced, ces métriques ne peuvent pas être consultées. Pour plus d'informations, voir AWS WAF métriques et dimensions.

Gestion de l'atténuation automatique des attaques DDoS au niveau de l'application

Suivez les instructions de cette section pour gérer les configurations d'atténuation automatique des attaques DDoS au niveau de la couche application. Pour plus d'informations sur le fonctionnement de l'atténuation automatique, consultez les rubriques précédentes.

> **Note**
>
> Suivez les meilleures pratiques décrites surBonnes pratiques pour l'utilisation de l'atténuation automatique.

Rubriques

- Affichage de la configuration d'atténuation automatique des attaques DDoS au niveau de la couche d'application pour une ressource
- Activation et désactivation de l'atténuation automatique des attaques DDoS au niveau de la couche applicative
- Modification de l'action utilisée pour l'atténuation automatique des attaques DDoS au niveau de la couche applicative
- Utilisation AWS CloudFormation avec atténuation automatique des attaques DDoS au niveau de la couche applicative

Affichage de la configuration d'atténuation automatique des attaques DDoS au niveau de la couche d'application pour une ressource

Vous pouvez consulter la configuration automatique de l'atténuation des attaques DDoS au niveau de la couche application pour une ressource sur la page Ressources protégées et sur les pages de protection individuelles.

Pour consulter la configuration automatique de l'atténuation des attaques DDoS au niveau de la couche d'application

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet AWS Shield de navigation, sélectionnez Ressources protégées. Dans la liste des ressources protégées, la colonne Atténuation automatique des attaques DDoS au niveau de la couche d'application indique si l'atténuation automatique est activée et, le cas échéant, l'action que Shield Advanced doit utiliser pour ses mesures d'atténuation.

   Vous pouvez également sélectionner n'importe quelle ressource de la couche application pour voir les mêmes informations répertoriées sur la page de protection de la ressource.

Activation et désactivation de l'atténuation automatique des attaques DDoS au niveau de la couche applicative

La procédure suivante indique comment activer ou désactiver la réponse automatique pour une ressource protégée.

Pour activer ou désactiver l'atténuation automatique des attaques DDoS au niveau de la couche application pour une seule ressource

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet AWS Shield de navigation, sélectionnez Ressources protégées.
3. Dans l'onglet Protections, sélectionnez la ressource de couche d'application pour laquelle vous souhaitez activer l'atténuation automatique. La page de protection de la ressource s'ouvre.
4. Sur la page de protection de la ressource, choisissez Modifier.
5. Sur la page Configurer l'atténuation des attaques DDoS de la couche 7 pour les ressources globales (facultatif), dans Atténuation automatique des attaques DDoS au niveau de la couche

application, choisissez l'option que vous souhaitez utiliser pour les atténuations automatiques. Les options de la console sont les suivantes :

- Conserver les paramètres actuels : n'apportez aucune modification aux paramètres d'atténuation automatique de la ressource protégée.
- Activer — Activez l'atténuation automatique pour la ressource protégée. Lorsque vous choisissez cette option, sélectionnez également l'action de règle que vous souhaitez que les atténuations automatiques utilisent dans les règles ACL Web. Pour plus d'informations sur les paramètres d'action des règles, consultezAction de la règle.

  Si votre ressource protégée n'a pas encore d'historique du trafic normal des applications, activez l'atténuation automatique en Count mode jusqu'à ce que Shield Advanced puisse établir une base de référence. Shield Advanced commence à collecter des informations pour sa base de référence lorsque vous associez une ACL Web à votre ressource protégée, et l'établissement d'une bonne base de trafic normal peut prendre de 24 heures à 30 jours.
- Désactiver : désactive l'atténuation automatique pour la ressource protégée.

6. Parcourez le reste des pages jusqu'à ce que vous ayez terminé et enregistrez la configuration.

Sur la page Protections, les paramètres d'atténuation automatique sont mis à jour pour la ressource.

Modification de l'action utilisée pour l'atténuation automatique des attaques DDoS au niveau de la couche applicative

Vous pouvez modifier l'action utilisée par Shield Advanced pour sa réponse automatique de la couche application à plusieurs emplacements de la console :

- Configuration de l'atténuation automatique : modifiez l'action lorsque vous configurez l'atténuation automatique pour votre ressource. Pour la procédure, reportez-vous à la section précédenteActivation et désactivation de l'atténuation automatique des attaques DDoS au niveau de la couche applicative.
- Page de détails de l'événement : modifiez l'action dans la page des détails de l'événement lorsque vous consultez les informations relatives à l'événement dans la console. Pour plus d'informations, consultez AWS Shield Advanced détails de l'événement.

Si vous avez deux ressources protégées qui partagent une ACL Web et que vous définissez l'action sur l'une et Count Block pour l'autre, Shield Advanced définit l'action de la règle `ShieldKnownOffenderIPRateBasedRule` basée sur le taux du groupe de règles sur. Block

Utilisation AWS CloudFormation avec atténuation automatique des attaques DDoS au niveau de la couche applicative

Découvrez comment utiliser pour AWS CloudFormation gérer vos protections et vos ACL AWS WAF Web.

Activation ou désactivation de l'atténuation automatique des attaques DDoS au niveau de la couche applicative

Vous pouvez activer et désactiver l'atténuation automatique des attaques DDoS au AWS CloudFormation niveau de la couche application en utilisant la `AWS::Shield::Protection` ressource. L'effet est le même que lorsque vous activez ou désactivez la fonctionnalité via la console ou toute autre interface. Pour plus d'informations sur AWS CloudFormation cette ressource, reportez-vous AWS::Shield::Protectionau guide de l'AWS CloudFormation utilisateur.

Gestion des ACL Web utilisées avec atténuation automatique

Shield Advanced gère l'atténuation automatique de votre ressource protégée à l'aide d'une règle de groupe de règles dans l'ACL AWS WAF Web de la ressource protégée. Par le biais de la AWS WAF console et des API, vous verrez la règle répertoriée dans vos règles ACL Web, avec un nom commençant par`ShieldMitigationRuleGroup`. Cette règle est dédiée à l'atténuation automatique des attaques DDoS au niveau de la couche applicative et est gérée pour vous par Shield Advanced et AWS WAF. Pour plus d’informations, consultez Le groupe de règles Shield Advanced et Comment Shield Advanced gère l'atténuation automatique.

Si vous avez l' AWS CloudFormation habitude de gérer vos ACL Web, n'ajoutez pas la règle de groupe de règles Shield Advanced à votre modèle d'ACL Web. Lorsque vous mettez à jour une ACL Web qui est utilisée avec vos protections d'atténuation automatiques, gère AWS WAF automatiquement la règle du groupe de règles dans l'ACL Web.

Vous constaterez les différences suivantes par rapport aux autres ACL Web par le biais AWS CloudFormation desquelles vous gérez :

- AWS CloudFormation ne signalera aucune dérive de l'état de dérive de la pile entre la configuration réelle de l'ACL Web, avec la règle du groupe de règles Shield Advanced, et votre modèle d'ACL Web, sans la règle. La règle Shield Advanced n'apparaîtra pas dans la liste réelle de la ressource dans les détails de dérive.

  Vous pourrez voir la règle du groupe de règles Shield Advanced dans les listes d'ACL Web que vous recherchez AWS WAF, par exemple via la AWS WAF console ou les AWS WAF API.

- Si vous modifiez le modèle d'ACL Web dans une pile AWS WAF et que Shield Advanced conserve automatiquement la règle d'atténuation automatique Shield Advanced dans l'ACL Web mise à jour. Les protections d'atténuation automatiques fournies par Shield Advanced ne sont pas interrompues par votre mise à jour de l'ACL Web.

Ne gérez pas la règle Shield Advanced dans votre modèle ACL AWS CloudFormation Web. Le modèle ACL Web ne doit pas répertorier la règle Shield Advanced. Suivez les meilleures pratiques en matière de gestion des ACL Web à l'adresseBonnes pratiques pour l'utilisation de l'atténuation automatique.

Détection basée sur l'état de santé au moyen de bilans

Vous pouvez configurer Shield Advanced pour utiliser la détection basée sur l'état de santé afin d'améliorer la réactivité et la précision de la détection et de l'atténuation des attaques. Vous pouvez utiliser cette option avec n'importe quel type de ressource, à l'exception des zones hébergées Route 53.

Pour configurer la détection basée sur l'état de santé, vous définissez un bilan de santé pour votre ressource dans Route 53, vous vérifiez qu'elle indique qu'elle est saine, puis vous l'associez à votre protection Shield Advanced. Pour plus d'informations sur les bilans de santé de Route 53, consultez Comment Amazon Route 53 vérifie l'état de vos ressources et Création, mise à jour et suppression de bilans de santé dans le guide du développeur Amazon Route 53.

> **Note**
>
> Des bilans de santé sont requis pour le support d'engagement proactif de la Shield Response Team (SRT). Pour plus d'informations sur l'engagement proactif, consultezConfiguration de l'engagement proactif.

Les bilans de santé mesurent l'état de santé de vos ressources en fonction des exigences que vous définissez. L'état du bilan de santé fournit des informations essentielles aux mécanismes de détection Shield Advanced, leur conférant une plus grande sensibilité à l'état actuel de vos applications spécifiques.

Vous pouvez activer la détection basée sur l'état de santé pour tous les types de ressources, à l'exception des zones hébergées Route 53.

- Ressources du réseau et de la couche transport (couche 3/couche 4) : la détection basée sur l'intégrité améliore la précision de la détection et de l'atténuation des événements au niveau des couches réseau et transport pour les équilibreurs de charge réseau, les adresses IP élastiques et les accélérateurs standard Global Accelerator. Lorsque vous protégez ces types de ressources avec Shield Advanced, Shield Advanced peut atténuer les attaques de moindre envergure et atténuer plus rapidement les attaques, même lorsque le trafic est dans les limites des capacités de l'application.

  Lorsque vous ajoutez une détection basée sur l'état de santé, pendant les périodes où le bilan de santé associé n'est pas satisfaisant, Shield Advanced peut appliquer des mesures d'atténuation encore plus rapidement et à des seuils encore plus bas.
- Ressources de la couche application (couche 7) : la détection basée sur l'état de santé améliore la précision de la détection des inondations de requêtes Web pour les CloudFront distributions et les équilibreurs de charge des applications. Lorsque vous protégez ces types de ressources avec Shield Advanced, vous recevez des alertes de détection des inondations de requêtes Web en cas d'écart statistiquement significatif du volume de trafic combiné à des modifications importantes des modèles de trafic, en fonction des caractéristiques des demandes.

  Grâce à la détection basée sur l'état de santé, lorsque le bilan de santé associé à Route 53 ne fonctionne pas correctement, Shield Advanced nécessite des écarts minimes pour alerter et signale les événements plus rapidement. À l'inverse, lorsque le bilan de santé associé à Route 53 est sain, Shield Advanced nécessite des écarts plus importants pour émettre une alerte.

Table des matières

- Équilibreurs de charge
- Adresse IP élastique (EIP) Amazon EC2

Bonnes pratiques pour l'utilisation des contrôles de santé avec Shield Advanced

Suivez les meilleures pratiques décrites dans cette section lorsque vous créez et utilisez des tests de santé avec Shield Advanced.

- Planifiez vos bilans de santé en identifiant les composants de votre infrastructure que vous souhaitez surveiller. Tenez compte des types de ressources suivants pour les bilans de santé :
  - Ressources critiques.
  - Toutes les ressources pour lesquelles vous souhaitez une plus grande sensibilité dans le cadre de la détection et de l'atténuation Shield Advanced.
  - Ressources pour lesquelles vous souhaitez que Shield Advanced vous contacte de manière proactive. L'engagement proactif est influencé par l'état de vos bilans de santé.

  Parmi les ressources que vous souhaiterez peut-être surveiller, citons les CloudFront distributions Amazon, les équilibreurs de charge connectés à Internet et les instances Amazon EC2.
- Définissez des contrôles de santé qui reflètent avec précision l'état de santé de l'origine de votre application avec le moins de notifications possible.
  - Rédigez des bilans de santé de manière à ce qu'ils ne soient défectueux que lorsque votre application n'est pas disponible ou ne fonctionne pas selon les paramètres acceptables. Vous êtes responsable de définir et de maintenir les bilans de santé en fonction des exigences spécifiques de votre application.
  - Effectuez le moins de bilans de santé possible tout en fournissant des rapports précis sur l'état de santé de votre application. Par exemple, plusieurs alarmes provenant de plusieurs domaines de votre application qui signalent toutes le même problème peuvent alourdir vos activités de réponse sans ajouter de valeur informative.
  - Utilisez des bilans de santé calculés pour surveiller l'état de santé des applications à l'aide d'une combinaison de CloudWatch mesures Amazon. Par exemple, vous pouvez calculer l'état de santé combiné en fonction de la latence de vos serveurs d'applications et de leurs taux d'erreur 5xx, ce qui indique que le serveur d'origine n'a pas répondu à la demande.
  - Créez et publiez vos propres indicateurs de santé des applications sous forme de métriques CloudWatch personnalisées selon les besoins et utilisez-les dans un bilan de santé calculé.

- Mettez en œuvre et gérez vos bilans de santé afin d'améliorer la détection et de réduire les activités de maintenance inutiles.
  - Avant d'associer un bilan de santé à une protection Shield Advanced, assurez-vous qu'elle est en bon état. Associer un bilan de santé signalant un dysfonctionnement peut fausser les mécanismes de détection de Shield Advanced pour vos ressources protégées.
  - Gardez vos bilans de santé à la disposition de Shield Advanced. Ne supprimez pas un bilan de santé dans Route 53 que vous utilisez pour une protection Shield Advanced.
  - Utilisez des environnements de test et de test uniquement pour tester vos bilans de santé. Conservez les associations de contrôle de santé uniquement pour les environnements nécessitant des performances et une disponibilité au niveau de la production. Ne maintenez pas l'association entre les contrôles de santé dans Shield Advanced pour les environnements de préparation et de test.

Métriques couramment utilisées pour les bilans de santé

Cette section répertorie les CloudWatch métriques Amazon couramment utilisées dans les bilans de santé pour mesurer l'état des applications lors d'événements de déni de service distribué (DDoS). Pour obtenir des informations complètes sur les CloudWatch mesures pour chaque type de ressource, consultez la liste qui suit le tableau.

Rubriques

Métriques utilisées pour surveiller l'état de santé des applications

Ressource	Métrique	Description
Route 53	`HealthCheckStatus`	État du point de terminaison du bilan de santé.
CloudFront	`5xxErrorRate`	Pourcentage de toutes les demandes pour lesquelles le code d'état HTTP est 5xx. Cela indique une attaque qui a un impact sur l'application.

Ressource	Métrique	Description
Application Load Balancer	`HTTPCode_ELB_5XX_Count`	Nombre de codes d'erreur client HTTP 5xx générés par l'équilibreur de charge.
Application Load Balancer	`RejectedConnectionCount`	Nombre de connexions rejetées parce que l'équilibreur de charge a atteint son nombre maximal de connexions.
Application Load Balancer	`TargetConnectionErrorCount`	Nombre de connexions qui n'ont pas été établies avec succès entre l'équilibreur de charge et la cible.
Application Load Balancer	`TargetResponseTime`	Temps écoulé en secondes après que la demande a quitté l'équilibreur de charge et lorsqu'elle a reçu une réponse de la cible.
Application Load Balancer	`UnHealthyHostCount`	Nombre de cibles considérées non saines.
Amazon EC2	`CPUUtilization`	Pourcentage d'unités de calcul EC2 allouées actuellement utilisées.

Statistiques CloudWatch Amazon pour chaque type de ressource

Pour plus d'informations sur les mesures disponibles pour vos ressources protégées, consultez les sections suivantes des guides de ressources :

- Amazon Route 53 — Surveillez vos ressources grâce aux bilans de santé d'Amazon Route 53 et CloudWatch à Amazon dans le guide du développeur Amazon Route 53.

- Amazon CloudFront — La surveillance CloudFront avec Amazon est décrite CloudWatch dans le manuel Amazon CloudFront Developer Guide.
- Application Load Balancer : CloudWatch indicateurs relatifs à votre Application Load Balancer dans le guide d'utilisation des Application Load Balancer.
- Network Load Balancer : CloudWatch indicateurs relatifs à votre Network Load Balancer dans le guide de l'utilisateur pour les Network Load Balancers.
- AWS Global Accelerator — Utilisation CloudWatch d'Amazon AWS Global Accelerator dans le manuel du AWS Global Accelerator développeur.
- Amazon Elastic Compute Cloud — Répertoriez les CloudWatch métriques disponibles pour vos instances sur le site https://docs.aws.amazon.com/ AWSEC 2/latest/ /. UserGuide
- Amazon EC2 Auto Scaling — Surveillance des CloudWatch métriques pour vos groupes et instances Auto Scaling dans le guide de l'utilisateur d'Amazon EC2 Auto Scaling.

Gestion des associations de bilans de santé

L'utilisation d'un bilan de santé avec Shield Advanced vous sera particulièrement utile si le bilan de santé indique uniquement que votre application fonctionne selon des paramètres acceptables et qu'il ne l'est pas lorsque ce n'est pas le cas. Suivez les instructions de cette section pour gérer vos associations de bilans de santé dans Shield Advanced.

> **Note**
>
> Shield Advanced ne gère pas automatiquement vos bilans de santé.

Les éléments suivants sont nécessaires pour utiliser un bilan de santé avec Shield Advanced :

- Le bilan de santé doit indiquer qu'il est sain lorsque vous l'associez à votre protection Shield Advanced.
- Le bilan de santé doit être pertinent par rapport à l'état de santé de votre ressource protégée. Vous êtes responsable de définir et de maintenir des bilans de santé qui indiquent avec précision l'état de santé de votre application, en fonction des exigences spécifiques de votre application.
- Le bilan de santé doit rester disponible pour être utilisé par la protection Shield Advanced. Ne supprimez pas un bilan de santé dans Route 53 que vous utilisez pour une protection Shield Advanced.

Rubriques

Associer un bilan de santé à votre ressource

La procédure suivante explique comment associer un bilan de santé Amazon Route 53 à une ressource protégée.

> **Note**
>
> Avant d'associer un bilan de santé à une protection Shield Advanced, assurez-vous qu'elle est en bon état. Pour plus d'informations, consultez la section Surveillance de l'état du bilan de santé et réception de notifications dans le guide du développeur Amazon Route 53.

Pour associer un bilan de santé

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet AWS Shield de navigation, sélectionnez Ressources protégées.
3. Dans l'onglet Protections, sélectionnez la ressource que vous souhaitez associer à un bilan de santé.
4. Choisissez Configurer les protections.
5. Choisissez Suivant jusqu'à ce que vous arriviez à la page Configurer la détection DDoS basée sur le contrôle de santé (facultatif).
6. Sous Associated Health Check (Vérification de l’état de santé associée), choisissez l'ID de la vérification de l’état de santé que vous souhaitez associer à la protection.

   > **Note**
   >
   > Si le bilan de santé dont vous avez besoin ne s'affiche pas, accédez à la console Route 53 et vérifiez le bilan de santé et son identifiant. Pour plus d'informations, consultez Creating and Updating Health Checks (Création et mise à jour des vérifications de l’état de santé).

7. Parcourez le reste des pages jusqu'à ce que vous ayez terminé la configuration. Sur la page Protections, votre association de contrôle de santé mise à jour est répertoriée pour la ressource.
8. Sur la page Protections, vérifiez que le bilan de santé que vous venez d'associer indique que vous êtes en bonne santé.

   Vous ne pouvez pas commencer à utiliser un bilan de santé dans Shield Advanced alors que celui-ci indique un dysfonctionnement. Cela permet à Shield Advanced de détecter les faux positifs à des seuils très bas et peut également avoir un impact négatif sur la capacité de la Shield Response Team (SRT) à impliquer de manière proactive la ressource.

   Si le nouveau bilan de santé associé indique un état insalubre, procédez comme suit :

   a. Dissociez le bilan de santé de votre protection dans Shield Advanced.
   b. Consultez les spécifications de votre bilan de santé dans Amazon Route 53 et vérifiez les performances et la disponibilité globales de vos applications.
   c. Lorsque les performances de votre application sont conformes à vos paramètres de santé et que votre bilan de santé indique qu'il est bon, essayez à nouveau d'associer le bilan de santé dans Shield Advanced.

La procédure d'association de bilans de santé est terminée lorsque vous avez créé votre nouvelle association de bilans de santé et qu'elle indique qu'elle est saine dans Shield Advanced.

Dissocier un bilan de santé de votre ressource

La procédure suivante explique comment dissocier un bilan de santé Amazon Route 53 d'une ressource protégée.

Pour dissocier un bilan de santé

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet AWS Shield de navigation, sélectionnez Ressources protégées.
3. Dans l'onglet Protections, sélectionnez la ressource que vous souhaitez dissocier d'un bilan de santé.
4. Choisissez Configurer les protections.
5. Choisissez Suivant jusqu'à ce que vous arriviez à la page Configurer la détection DDoS basée sur le contrôle de santé (facultatif).

6. Sous Associated Health Check, choisissez l'option vide, répertoriée sous la forme -.
7. Parcourez le reste des pages jusqu'à ce que vous ayez terminé la configuration.

Sur la page Protections, le champ de vérification de l'état de votre ressource est défini sur -, ce qui indique qu'il n'y a aucune association avec le bilan de santé.

Le statut de l'association de bilans de santé

Vous pouvez consulter l'état du bilan de santé associé à une protection sur la page des ressources protégées de la console AWS WAF & Shield et sur la page de détails de chaque ressource.

- En bonne santé — Le bilan de santé est disponible et indique que vous êtes en bonne santé.
- Malsain — Le bilan de santé est disponible et indique un état de santé malsain.
- Non disponible — Le bilan de santé n'est pas disponible pour Shield Advanced.

Pour résoudre un bilan de santé non disponible

Créez et utilisez un nouveau bilan de santé. N'essayez pas d'associer à nouveau un bilan de santé lorsqu'il est devenu indisponible dans Shield Advanced.

Pour obtenir des instructions détaillées sur la manière de suivre ces étapes, consultez les rubriques précédentes.

1. Dans Shield Advanced, dissociez le bilan de santé de la ressource.
2. Dans Route 53, créez un nouveau bilan de santé pour la ressource et notez son identifiant. Pour plus d'informations, consultez Creating and Updating Health Checks dans le manuel Amazon Route 53 Developer Guide.
3. Dans Shield Advanced, associez le nouveau bilan de santé à la ressource.

Exemples de bilans de santé

Cette section présente des exemples de bilans de santé que vous pourriez utiliser dans un bilan de santé calculé. Un bilan de santé calculé utilise un certain nombre de bilans de santé individuels pour déterminer un statut combiné. Le statut de chaque bilan de santé individuel est basé sur l'état d'un terminal ou sur l'état d'une CloudWatch métrique Amazon. Vous combinez les bilans de santé dans un bilan de santé calculé, puis vous configurez votre bilan de santé calculé pour signaler l'état de santé en fonction de l'état de santé combiné des bilans de santé individuels. Ajustez la sensibilité

de vos bilans de santé calculés en fonction de vos exigences en matière de performances et de disponibilité des applications.

Pour plus d'informations sur les bilans de santé calculés, consultez la section Surveillance des autres bilans de santé (bilans de santé calculés) dans le manuel Amazon Route 53 Developer Guide. Pour plus d'informations, consultez le billet de blog Améliorations de Route 53 — Calculated Health Checks and Latency Checks.

Rubriques

- CloudFront Distributions Amazon
- Équilibreurs de charge
- Adresse IP élastique (EIP) Amazon EC2

CloudFront Distributions Amazon

Les exemples suivants décrivent les bilans de santé qui peuvent être combinés dans un bilan de santé calculé pour une CloudFront distribution :

- Surveillez un point de terminaison en spécifiant un nom de domaine vers un chemin sur la distribution qui diffuse du contenu dynamique. Une réponse saine inclurait les codes de réponse HTTP 2xx et 3xx.
- Surveillez l'état d'une CloudWatch alarme qui mesure l'état de santé de CloudFront son origine. Par exemple, vous pouvez maintenir une CloudWatch alarme sur la métrique `TargetResponseTime` Application Load Balancer et créer un bilan de santé qui reflète l'état de l'alarme. Le bilan de santé peut être défaillant lorsque le temps de réponse, entre la demande quittant l'équilibreur de charge et le moment où l'équilibreur de charge reçoit une réponse de la cible, dépasse le seuil configuré dans l'alarme.
- Surveillez l'état d'une CloudWatch alarme qui mesure le pourcentage de demandes pour lesquelles le code d'état HTTP de la réponse est 5xx. Si le taux d'erreur 5xx de la CloudFront distribution est supérieur au seuil défini dans l' CloudWatch alarme, le statut de ce bilan de santé passe en état de mauvais état.

Équilibreurs de charge

Les exemples suivants décrivent les contrôles de santé qui peuvent être utilisés dans les contrôles de santé calculés pour un accélérateur standard Application Load Balancer, Network Load Balancer ou Global Accelerator.

- Surveillez l'état d'une CloudWatch alarme qui mesure le nombre de nouvelles connexions établies par les clients à l'équilibreur de charge. Vous pouvez définir le seuil d'alarme pour le nombre moyen de nouvelles connexions à un certain degré supérieur à votre moyenne quotidienne. Les mesures pour chaque type de ressource sont les suivantes :
  - Application Load Balancer : `NewConnectionCount`
  - Network Load Balancer : `ActiveFlowCount`
  - Accélérateur mondial : `NewFlowCount`
- Pour Application Load Balancer et Network Load Balancer, surveillez l'état d' CloudWatch une alarme qui mesure le nombre d'équilibreurs de charge considérés comme sains. Vous pouvez définir le seuil d'alarme soit sur la zone de disponibilité, soit sur le nombre minimum d'hôtes sains requis par votre équilibreur de charge. Les mesures disponibles pour les ressources de l'équilibreur de charge sont les suivantes :
  - Application Load Balancer : `HealthyHostCount`
  - Network Load Balancer : `HealthyHostCount`
- Pour Application Load Balancer, surveillez l'état d'une CloudWatch alarme qui mesure le nombre de codes de réponse HTTP 5xx générés par les cibles de l'équilibreur de charge. Pour un Application Load Balancer, vous pouvez utiliser la métrique `HTTPCode_Target_5XX_Count` et baser le seuil d'alarme sur la somme des erreurs 5xx de l'équilibreur de charge.

Adresse IP élastique (EIP) Amazon EC2

Les exemples de tests de santé suivants peuvent être combinés dans un contrôle de santé calculé pour une adresse IP élastique Amazon EC2 :

- Surveillez un point de terminaison en spécifiant une adresse IP pour l'adresse IP élastique. Le bilan de santé restera sain tant qu'une connexion TCP pourra être établie avec la ressource qui se trouve derrière l'adresse IP.
- Surveillez l'état d'une CloudWatch alarme qui mesure le pourcentage d'unités de calcul Amazon EC2 allouées actuellement utilisées sur l'instance. Vous pouvez utiliser la métrique Amazon EC2 `CPUUtilization` et baser le seuil d'alarme sur ce que vous considérez comme un taux d'utilisation du processeur élevé pour votre application, tel que 90 %.

Gestion de la protection des ressources dans AWS Shield Advanced

Suivez les instructions de cette section pour gérer les protections Shield Advanced pour vos ressources.

> **Note**
>
> Shield Advanced protège uniquement les ressources que vous avez spécifiées soit dans Shield Advanced, soit par le biais d'une politique AWS Firewall Manager Shield Advanced. Il ne protège pas automatiquement vos ressources.

Si vous utilisez une politique AWS Firewall Manager Shield Advanced, vous n'avez pas besoin de gérer la protection des ressources couvertes par cette politique. Firewall Manager gère automatiquement les protections des comptes et des ressources concernés par une politique, conformément à la configuration de la politique. Pour plus d'informations, consultez AWS Shield Advanced politiques.

Rubriques

- Ajouter AWS Shield Advanced une protection aux AWS ressources
- Configuration des AWS Shield Advanced protections
- Supprimer AWS Shield Advanced la protection d'une AWS ressource

Ajouter AWS Shield Advanced une protection aux AWS ressources

Suivez les instructions de cette section pour ajouter la protection Shield Advanced à une ou plusieurs ressources.

Pour ajouter une protection à une AWS ressource

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet de navigation, sous AWS Shield Choisissez Ressources protégées.
3. Choisissez Ajouter des ressources à protéger.
4. Sur la page Choisissez les ressources à protéger avec Shield Advanced, dans Spécifiez la région et les types de ressources, indiquez les spécifications de région et de type de ressource

pour les ressources que vous souhaitez protéger. Vous pouvez protéger les ressources de plusieurs régions en sélectionnant Toutes les régions et vous pouvez restreindre la sélection aux ressources mondiales en sélectionnant Global. Vous pouvez désélectionner les types de ressources que vous ne souhaitez pas protéger. Pour plus d'informations sur les protections de vos types de ressources, consultezAWS Shield Advanced protections par type de ressource.

5. Choisissez Charger les ressources. Shield Advanced renseigne la section Select Resources avec les AWS ressources correspondant à vos critères.
6. Dans la section Sélectionner les ressources, vous pouvez filtrer la liste des ressources en saisissant une chaîne à rechercher dans les listes de ressources.

   Sélectionnez les ressources que vous souhaitez protéger.
7. Dans la section Tags, si vous souhaitez ajouter des balises aux protections Shield Advanced que vous créez, spécifiez-les. Pour plus d'informations sur le balisage AWS des ressources, consultez la section Utilisation de l'éditeur de balises.
8. Choisissez Protect with Shield Advanced. Cela ajoute les protections Shield Advanced aux ressources.

Configuration des AWS Shield Advanced protections

Vous pouvez modifier les paramètres de vos AWS Shield Advanced protections à tout moment. Pour ce faire, parcourez les options correspondant aux protections que vous avez sélectionnées et modifiez les paramètres que vous devez modifier.

Pour gérer les ressources protégées

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet AWS Shield de navigation, sélectionnez Ressources protégées.
3. Dans l'onglet Protections, sélectionnez les ressources que vous souhaitez protéger.
4. Choisissez Configurer les protections et l'option de spécification des ressources que vous souhaitez.
5. Passez en revue chacune des options de protection des ressources et apportez les modifications nécessaires.

Configuration des protections DDoS au niveau de la couche applicative

Pour vous protéger contre les attaques visant les ressources Amazon CloudFront et Application Load Balancer, vous pouvez ajouter des ACL AWS WAF Web et des règles basées sur le taux. Pour plus d'informations à ce sujet, consultezShield Advanced, couche d'application, ACL AWS WAF Web et règles basées sur le débit.

Vous pouvez également activer l'atténuation automatique des attaques DDoS au niveau de la couche d'application Shield Advanced. Pour plus d'informations sur le AWS WAF fonctionnement, voirAWS WAF. Pour plus d'informations sur la fonction d'atténuation automatique, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

Important

Si vous gérez vos protections Shield Advanced à AWS Firewall Manager l'aide d'une politique Shield Advanced, vous ne pouvez pas gérer les protections de la couche application ici. Pour toutes les autres ressources, nous vous recommandons d'associer au minimum une ACL Web à chaque ressource, même si l'ACL Web ne contient aucune règle.

Note

Lorsque vous activez l'atténuation automatique des attaques DDoS au niveau de la couche application pour une ressource, si nécessaire, l'opération ajoute automatiquement un rôle lié à un service à votre compte afin de donner à Shield Advanced les autorisations dont il a besoin pour gérer vos protections ACL Web. Pour plus d’informations, consultez Utilisation de rôles liés à un service pour Shield Advanced.

Pour configurer les protections DDoS de la couche application

1. Sur la page Configurer les protections DDoS de la couche 7, si la ressource n'est pas déjà associée à une ACL Web, vous pouvez choisir une ACL Web existante ou créer la vôtre.

   Pour créer une liste ACL web, procédez comme suit :

   a. Sélectionnez Create web ACL.
   b. Entrez un nom. Vous ne pouvez pas modifier le nom une fois que vous créez la liste ACL web.

c. Choisissez Créer.

> **Note**
>
> Si une ressource est déjà associée à une liste ACL web, vous ne pouvez pas passer à une autre liste ACL web. Si vous souhaitez modifier la liste ACL web, vous devez d'abord supprimer les listes ACL web associées à partir de la ressource. Pour plus d'informations, consultez Associer ou dissocier une ACL Web à une ressource AWS.

2. Si aucune règle basée sur le taux n'est définie dans l'ACL Web, vous pouvez en ajouter une en choisissant Ajouter une règle de limite de débit, puis en effectuant les étapes suivantes :

   a. Entrez un nom.

   b. Entrez une limite de débit. Il s'agit du nombre maximum de demandes autorisées sur une période de cinq minutes à partir d'une adresse IP unique avant que l'action de la règle basée sur le taux ne soit appliquée à l'adresse IP. Lorsque les demandes provenant de l'adresse IP tombent en dessous de la limite, l'action est interrompue.

   c. Définissez l'action de règle pour compter ou bloquer les demandes provenant d'adresses IP lorsque le nombre de demandes dépasse la limite. L'action d'application et de suppression de la règle peut prendre effet une minute ou deux après la modification du taux de demandes d'adresse IP.

   d. Choisissez Ajouter une règle.

3. Pour l'atténuation automatique des attaques DDoS au niveau de la couche application, choisissez si vous souhaitez que Shield Advanced atténue automatiquement les attaques DDoS en votre nom, comme suit :

   - Pour activer l'atténuation automatique, choisissez Enable, puis sélectionnez l'action de AWS WAF règle que Shield Advanced doit utiliser dans ses règles personnalisées. Vos choix sont Count etBlock. Pour plus d'informations sur ces actions liées aux AWS WAF règles, consultezAction de la règle. Pour plus d'informations sur la façon dont Shield Advanced gère ce paramètre d'action, consultezComment Shield Advanced gère le paramètre d'action des règles.
   - Pour désactiver l'atténuation automatique, choisissez Désactiver.
   - Pour que les paramètres d'atténuation automatique restent inchangés pour les ressources que vous gérez, laissez le choix par défaut Conserver les paramètres actuels.

Pour plus d'informations sur l'atténuation automatique des attaques DDoS au niveau de la couche d'application Shield Advanced, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

4. Choisissez Suivant.

Créez des alarmes et des notifications

La procédure suivante indique comment gérer les CloudWatch alarmes relatives aux ressources protégées.

> **Note**
>
> CloudWatch entraîne des coûts supplémentaires. Pour CloudWatch connaître les tarifs, consultez Amazon CloudWatch Pricing.

Pour créer des alarmes et des notifications

1. Sur la page de protection Créer des alarmes et des notifications (facultatif), configurez les rubriques SNS pour les alarmes et les notifications que vous souhaitez recevoir. Pour les ressources pour lesquelles vous ne souhaitez pas de notifications, choisissez No topic (Aucune rubrique). Vous pouvez ajouter une rubrique Amazon SNS ou en créer une nouvelle.
2. Pour créer une rubrique Amazon SNS, procédez comme suit :
   a. Dans la liste déroulante, choisissez Créer une rubrique SNS.
   b. Saisissez un nom de rubrique.
   c. Entrez éventuellement une adresse e-mail à laquelle les messages Amazon SNS seront envoyés, puis choisissez Ajouter un e-mail. Vous pouvez en saisir plusieurs.
   d. Choisissez Créer.
3. Choisissez Suivant.

Supprimer AWS Shield Advanced la protection d'une AWS ressource

Vous pouvez supprimer AWS Shield Advanced la protection de n'importe laquelle de vos AWS ressources à tout moment.

> **Important**
>
> La suppression d'une AWS ressource n'entraîne pas la suppression de la ressource de AWS Shield Advanced. Vous devez également supprimer la protection de la ressource AWS Shield Advanced, comme décrit dans cette procédure.

Supprimer AWS Shield Advanced la protection d'une AWS ressource

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet AWS Shield de navigation, sélectionnez Ressources protégées.
3. Dans l'onglet Protections, sélectionnez les ressources dont vous souhaitez supprimer les protections.
4. Choisissez Supprimer les protections.

    - Si une CloudWatch alarme Amazon est configurée pour une protection, vous avez la possibilité de supprimer l'alarme en même temps que la protection. Si vous choisissez de ne pas supprimer l'alarme à ce stade, vous pouvez la supprimer ultérieurement à l'aide de la CloudWatch console.

    > **Note**
    >
    > Pour les protections pour lesquelles un bilan de santé Amazon Route 53 est configuré, si vous ajoutez à nouveau la protection ultérieurement, la protection inclut toujours le bilan de santé.

Les étapes précédentes suppriment AWS Shield Advanced la protection de AWS ressources spécifiques. Ils n'annulent pas votre AWS Shield Advanced abonnement. Le service continuera de vous être facturé. Pour plus d'informations sur votre AWS Shield Advanced abonnement, contactez le AWS Support Centre.

Supprimer une CloudWatch alarme de vos protections Shield Advanced

Pour supprimer une CloudWatch alarme de vos protections Shield Advanced, effectuez l'une des opérations suivantes :

- Supprimer la protection comme décrit dans Supprimer AWS Shield Advanced la protection d'une AWS ressource. Veillez à sélectionner la case à cocher en regard de Also delete related DDoSDetection alarm (Supprimer également l'alarme DDoSDetection associée).
- Supprimez l'alarme à l'aide de la CloudWatch console. Le nom de l'alarme à supprimer commence par DDoS DetectedAlarmForProtection.

AWS Shield Advanced groupes de protection

Utilisez des groupes de protection pour créer des collections logiques de vos ressources protégées et gérer leurs protections en tant que groupe. Pour plus d'informations sur la gestion de la protection des ressources, consultezConfiguration des AWS Shield Advanced protections.

> **Note**
>
> L'atténuation automatique des attaques DDoS au niveau de la couche applicative n'interagit pas avec les groupes de protection. Vous pouvez activer l'atténuation automatique pour les ressources appartenant à des groupes de protection, mais Shield Advanced n'applique pas automatiquement les mesures d'atténuation des attaques en fonction des résultats des groupes de protection. Shield Advanced applique des mesures d'atténuation automatiques des attaques pour les ressources individuelles.

AWS Shield Advanced les groupes de protection vous offrent un moyen en libre-service de personnaliser l'étendue de la détection et de l'atténuation en traitant plusieurs ressources protégées comme une seule unité. Le regroupement des ressources peut présenter de nombreux avantages.

- Améliorez la précision de détection.
- Réduisez les notifications d'événements non exploitables.
- Élargir la couverture des mesures d'atténuation afin d'inclure les ressources protégées qui pourraient également être affectées lors d'un événement.
- Accélérez le temps nécessaire pour atténuer les attaques visant plusieurs cibles similaires.
- Facilitez la protection automatique des ressources protégées nouvellement créées.

Les groupes de protection peuvent contribuer à réduire les faux positifs dans des situations telles que l'échange bleu/vert, où les ressources alternent entre une charge proche de zéro et une charge complète. Un autre exemple est celui où vous créez et supprimez fréquemment des ressources tout

en maintenant un niveau de charge partagé entre les membres du groupe. Dans de telles situations, la surveillance de ressources individuelles peut donner lieu à des faux positifs, ce qui n'est pas le cas de la surveillance de l'état du groupe de ressources.

Vous pouvez configurer les groupes de protection pour inclure toutes les ressources protégées, toutes les ressources de types de ressources spécifiques ou les ressources spécifiées individuellement. Les ressources nouvellement protégées qui répondent aux critères de votre groupe de protection sont automatiquement incluses dans votre groupe de protection. Une ressource protégée peut appartenir à plusieurs groupes de protection.

Gestion des groupes AWS Shield Advanced de protection

Suivez les instructions de cette section pour gérer les configurations de vos groupes de protection.

Création d'un groupe de protection Shield Advanced

Pour créer un groupe de protection

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet AWS Shield de navigation, sélectionnez Ressources protégées.
3. Choisissez l'onglet Groupes de protection, puis choisissez Créer un groupe de protection.
4. Sur la page Créer un groupe de protection, donnez un nom à votre groupe. Vous utiliserez ce nom pour identifier le groupe dans votre liste de ressources protégées. Vous ne pouvez pas modifier le nom d'un groupe de protection après l'avoir créé.
5. Pour les critères de regroupement de protection, sélectionnez les critères que Shield Advanced doit utiliser pour identifier les ressources protégées à inclure dans le groupe. Effectuez vos sélections supplémentaires en fonction des critères que vous avez choisis.
6. Pour l'agrégation, sélectionnez la manière dont vous souhaitez que Shield Advanced combine les données des ressources du groupe afin de détecter, d'atténuer et de signaler les événements.

   - Somme — Utilise le trafic total du groupe. C'est un bon choix dans la plupart des cas. Les exemples incluent les adresses IP élastiques pour les instances Amazon EC2 qui sont mises à l'échelle manuellement ou automatiquement.
   - Moyenne : utilisez la moyenne du trafic au sein du groupe. C'est un bon choix pour les ressources qui partagent le trafic de manière uniforme. Les accélérateurs et les équilibreurs de charge en sont des exemples.

- Max — Utilisez le trafic le plus élevé provenant de chaque ressource. Cela est utile pour les ressources qui ne partagent pas le trafic et pour les ressources qui partagent le trafic de manière non uniforme. Les exemples incluent les CloudFront distributions Amazon et les ressources d'origine pour les CloudFront distributions.

7. Choisissez Enregistrer pour enregistrer votre groupe de protection et revenir à la page Ressources protégées.

Sur la page Shield Events, vous pouvez consulter les événements relatifs à votre groupe de protection et effectuer une recherche détaillée pour obtenir des informations supplémentaires sur les ressources protégées du groupe.

Mettre à jour un groupe de protection Shield Advanced

Pour mettre à jour un groupe de protection

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet AWS Shield de navigation, sélectionnez Ressources protégées.
3. Dans l'onglet Groupes de protection, cochez la case à côté du groupe de protection que vous souhaitez modifier.
4. Sur la page du groupe de protection, choisissez Modifier. Apportez vos modifications aux paramètres du groupe de protection.
5. Choisissez Save pour enregistrer les changements.

Supprimer un groupe de protection Shield Advanced

Pour supprimer un groupe de protection

1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet AWS Shield de navigation, sélectionnez Ressources protégées.
3. Dans l'onglet Groupes de protection, cochez la case à côté du groupe de protection que vous souhaitez supprimer.
4. Sur la page du groupe de protection, choisissez Supprimer et confirmez l'action.

Suivi des modifications apportées à la protection des ressources dans AWS Config

Vous pouvez enregistrer les modifications apportées à la AWS Shield Advanced protection de vos ressources à l'aide de AWS Config. Vous pouvez ensuite utiliser ces informations pour conserver un historique des changements de configuration à des fins d'audit et de dépannage.

Pour enregistrer les modifications de protection, activez-les AWS Config pour chaque ressource que vous souhaitez suivre. Pour plus d'informations, consultez Mise en route avec AWS Config dans le AWS Config Guide du développeur.

Vous devez l'activer AWS Config pour chaque ressource Région AWS contenant les ressources suivies. Vous pouvez l'activer AWS Config manuellement ou utiliser le AWS CloudFormation modèle « Activer AWS Config » dans la section AWS CloudFormation StackSets Exemples de modèles du guide de l'AWS CloudFormation utilisateur.

Si vous l'activez AWS Config, vous êtes débité comme indiqué sur la page de AWS Config tarification.

> **Note**
>
> Si vous avez déjà AWS Config activé les régions et les ressources nécessaires, vous n'avez rien à faire. AWS Config les journaux concernant les modifications de protection apportées à vos ressources commencent à se remplir automatiquement.

Après l'activation AWS Config, utilisez la région USA Est (Virginie du Nord) dans la AWS Config console pour afficher l'historique des modifications de configuration des ressources AWS Shield Advanced globales.

Consultez l'historique des modifications des ressources AWS Shield Advanced régionales via la AWS Config console dans les régions USA Est (Virginie du Nord), USA Est (Ohio), USA Ouest (Oregon), USA Ouest (Californie du Nord), Europe (Irlande), Europe (Francfort), Asie-Pacifique (Tokyo) et Asie-Pacifique (Sydney).

Visibilité sur les événements DDoS

AWS Shield fournit de la visibilité sur les catégories d'événements et d'activités événementielles suivantes :

- Global — Tous les clients peuvent accéder à une vue agrégée de l'activité des menaces mondiales au cours des deux dernières semaines. Vous pouvez consulter ces informations sur les pages Getting Started et Global Threat Dashboard de la AWS Shield console. Pour plus d'informations, consultez AWS Shield activité globale et activité du compte.
- Compte — Tous les clients peuvent accéder à un résumé des événements liés à leur compte au cours de l'année précédente. Vous pouvez consulter ces informations sur la page Getting Started de la AWS Shield console. Pour plus d'informations, consultez AWS Shield activité globale et activité du compte.

Lorsque vous vous abonnez à Shield Advanced et que vous ajoutez des protections à vos ressources, vous avez accès à des informations supplémentaires sur les événements et les attaques DDoS visant les ressources protégées :

- Événements sur des ressources protégées : Shield Advanced fournit des informations détaillées sur chaque événement via la page Événements de la AWS Shield console. Pour plus d'informations, consultez AWS Shield Advanced événements.
- Mesures relatives aux événements pour les ressources protégées : Shield Advanced publie les CloudWatch statistiques Amazon relatives à la détection, à l'atténuation et aux principaux contributeurs pour toutes les ressources qu'elle protège. Vous pouvez utiliser ces métriques pour configurer des CloudWatch tableaux de bord et des alarmes. Pour plus d'informations, consultez AWS Shield Advanced métriques.
- Visibilité des événements entre comptes pour les ressources protégées — Si vous gérez vos protections Shield Advanced, vous pouvez activer la visibilité des protections sur plusieurs comptes en utilisant Firewall Manager associé AWS Security Hubà. AWS Firewall Manager Pour plus d'informations, consultez Visibilité des événements sur tous les comptes.

Si vous activez l'atténuation automatique des attaques DDoS au niveau de la couche application pour une protection de la couche application,

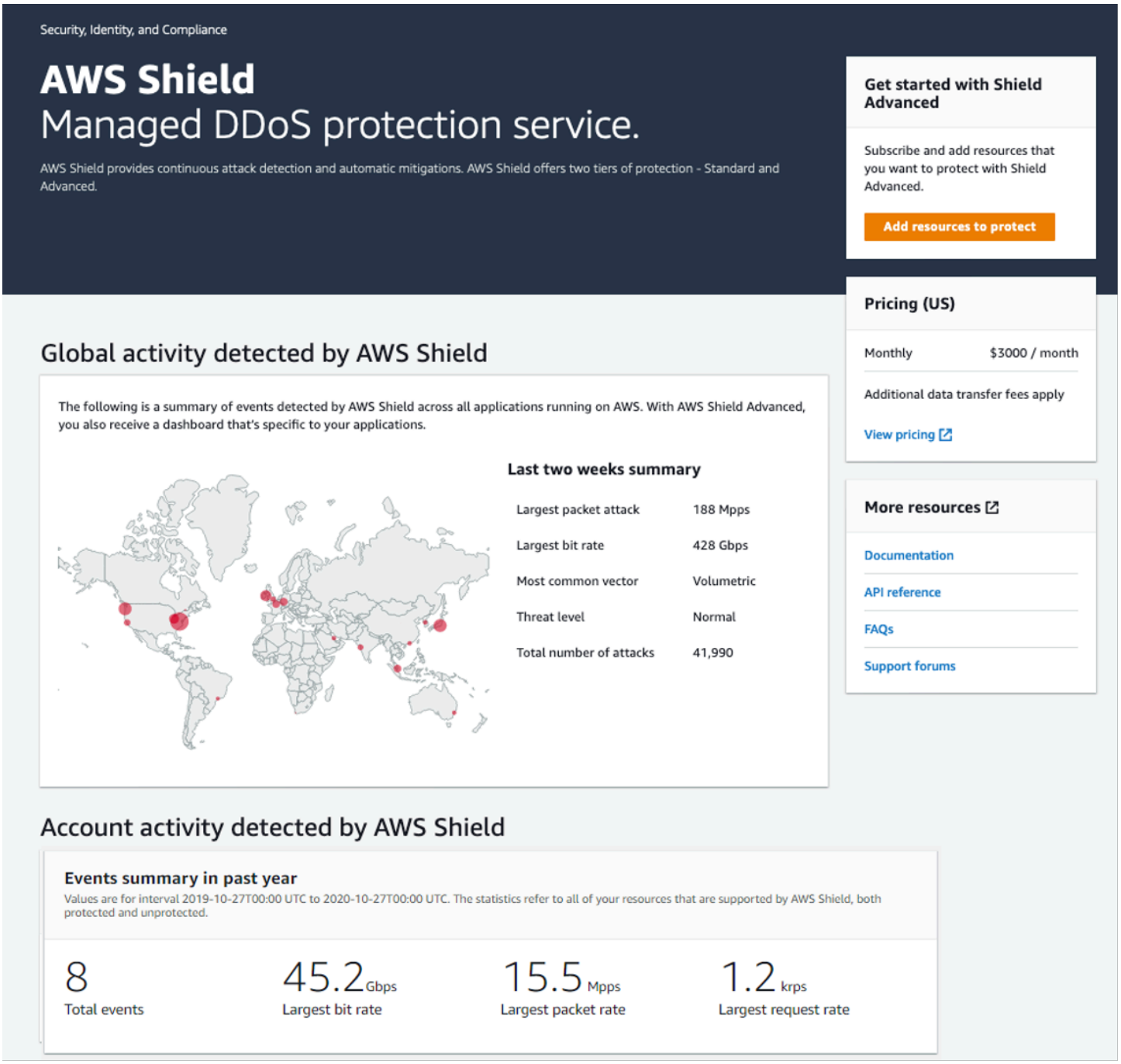
Rubriques

- AWS Shield activité globale et activité du compte
- AWS Shield Advanced événements
- Visibilité des événements sur tous les comptes

AWS Shield activité globale et activité du compte

Vous pouvez accéder à une vue agrégée de l'activité globale des menaces et à un résumé des événements par compte sur les pages Getting Started et Global Threat Dashboard de la AWS Shield console.

La capture d'écran suivante montre un exemple de page de démarrage.



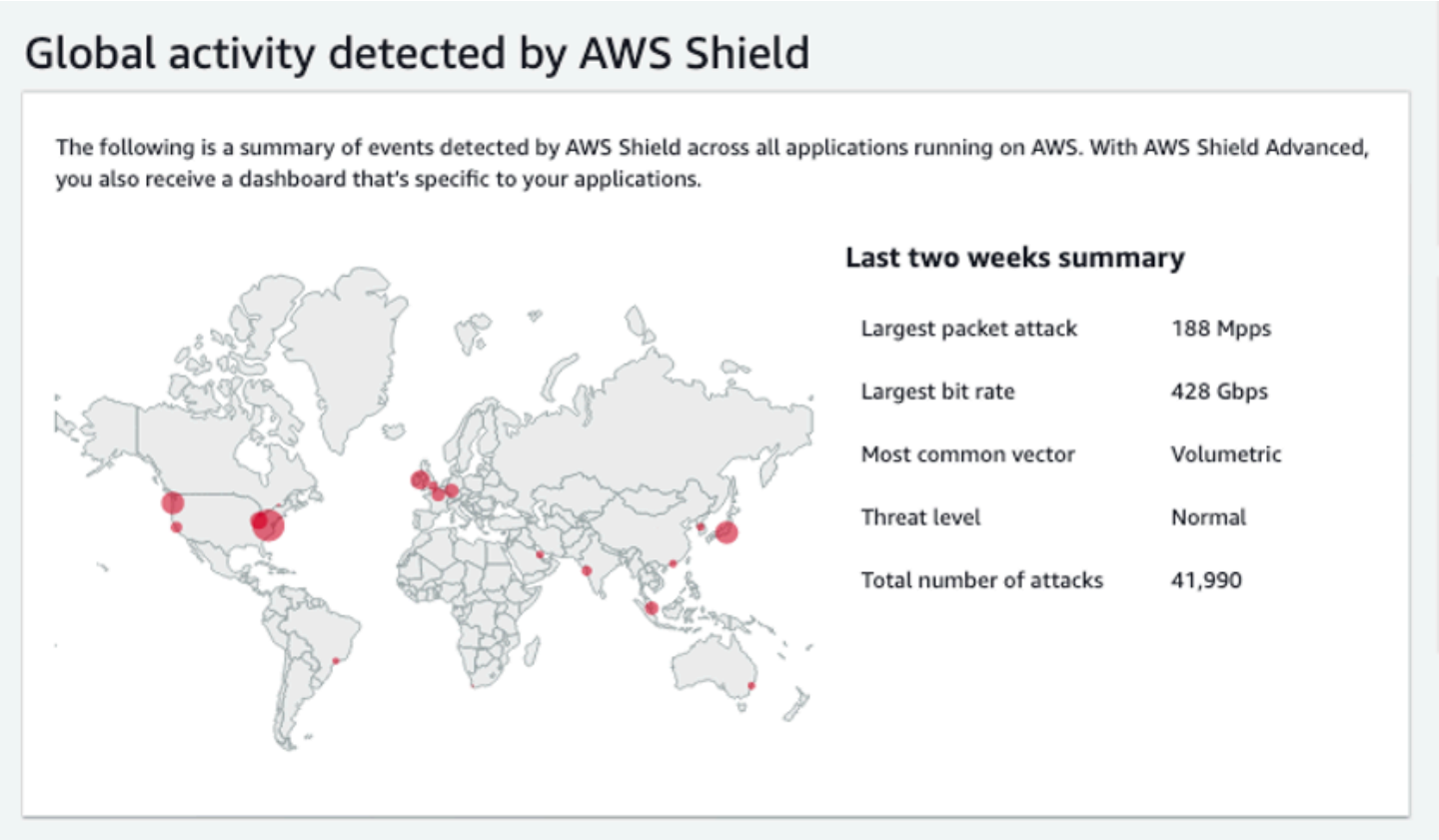
Pour accéder à la AWS Shield console

- Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.

Vous n'avez pas besoin d'un abonnement à Shield Advanced pour accéder aux informations récapitulatives sur l'activité globale et les événements du compte.

Activité mondiale

Ces informations sont disponibles via le tableau de bord des menaces mondiales de la AWS Shield console et les pages Getting Started. La capture d'écran suivante montre un exemple du volet d'activité global.



L'activité mondiale décrit les événements DDoS observés chez tous les AWS clients. Une fois par heure, AWS met à jour les informations des deux semaines précédentes. Dans le volet de la console, vous pouvez voir les résultats, partitionnés par AWS région et affichés sur une carte thermique mondiale. À côté de la carte, Shield affiche des informations récapitulatives telles que l'attaque de paquets la plus importante, le débit le plus élevé, le vecteur le plus courant, le nombre total d'attaques et le niveau de menace. Le niveau de menace est une évaluation de l'activité mondiale

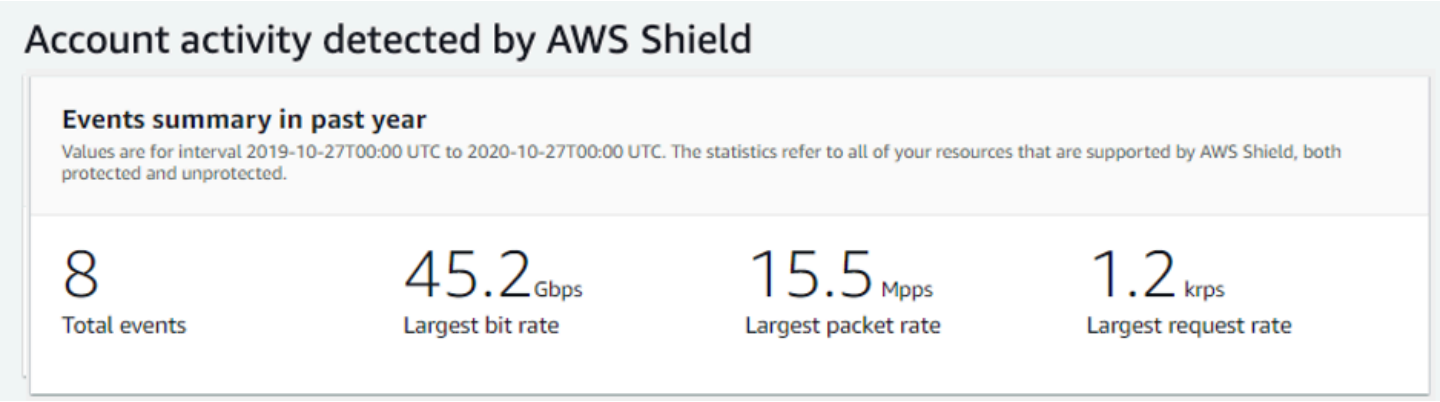
actuelle par rapport à ce qui est AWS généralement observé. La valeur du niveau de menace par défaut est Normal. AWS met automatiquement à jour la valeur sur Élevé en cas d'activité DDoS élevée.

Le tableau de bord des menaces mondiales fournit également des statistiques chronologiques et vous permet de changer de durée. Pour consulter l'historique des attaques DDoS importantes, vous pouvez personnaliser le tableau de bord en fonction des vues du dernier jour aux deux dernières semaines. Les métriques chronologiques fournissent une vue du débit binaire, du débit de paquets ou du débit de demandes le plus élevé pour tous les événements détectés par AWS Shield les applications exécutées AWS pendant la fenêtre temporelle que vous sélectionnez.

Activité du compte

Ces informations sont disponibles sur la page Getting AWS Shield Started de la console.

La capture d'écran suivante montre un exemple de volet d'activité du compte.



L'activité du compte décrit les événements DDoS détectés par Shield pour vos ressources éligibles à la protection de Shield Advanced. Chaque jour, Shield crée des statistiques récapitulatives pour l'année se terminant à 00h00 UTC la veille, puis affiche le total des événements, le débit binaire le plus élevé, le débit de paquets le plus élevé et le plus grand débit de demandes.

- L'indicateur du nombre total d'événements reflète chaque fois que Shield a détecté des attributs suspects dans le trafic destiné à votre application. Les attributs suspects peuvent inclure un trafic dont le volume est supérieur à la normale, le trafic qui ne correspond pas au profil historique de votre application ou le trafic qui ne correspond pas aux heuristiques définies par Shield pour le trafic d'applications valide.
- Les statistiques de débit et de débit de paquets les plus élevés sont disponibles pour chaque ressource.

- La statistique de taux de demande la plus importante n'est disponible que pour les CloudFront distributions Amazon et les équilibreurs de charge d'application associés à une ACL AWS WAF Web.

> **Note**
>
> Vous pouvez également accéder au résumé des événements au niveau du compte via l'opération AWS Shield API DescribeAttackStatistics.

AWS Shield Advanced événements

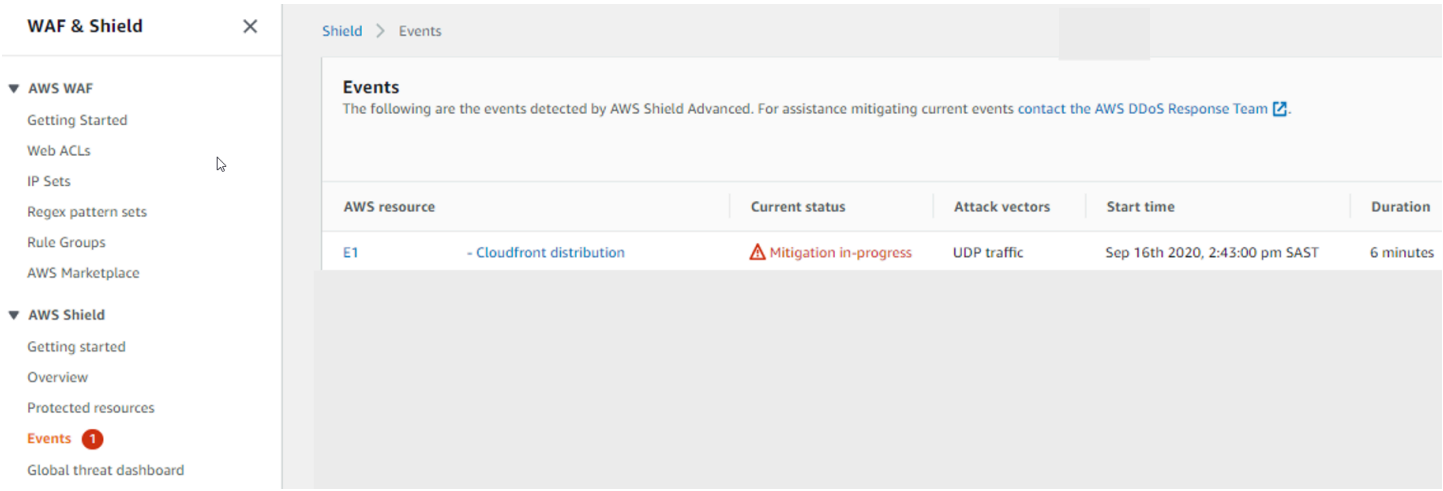
Lorsque vous vous abonnez à Shield Advanced et que vous protégez vos ressources, vous avez accès à des fonctionnalités de visibilité supplémentaires pour les ressources. Il s'agit notamment de la notification en temps quasi réel des événements détectés par Shield Advanced et d'informations supplémentaires sur les événements détectés et les mesures d'atténuation.

> **Note**
>
> Les informations relatives à vos événements dans la console Shield Advanced sont basées sur les métriques de Shield Advanced. Pour plus d'informations sur les métriques Shield Advanced, voir AWS Shield Advanced métriques

AWS Shield évalue le trafic vers votre ressource protégée selon plusieurs dimensions. Lorsqu'une anomalie est détectée, Shield Advanced crée un événement distinct pour chaque ressource affectée.

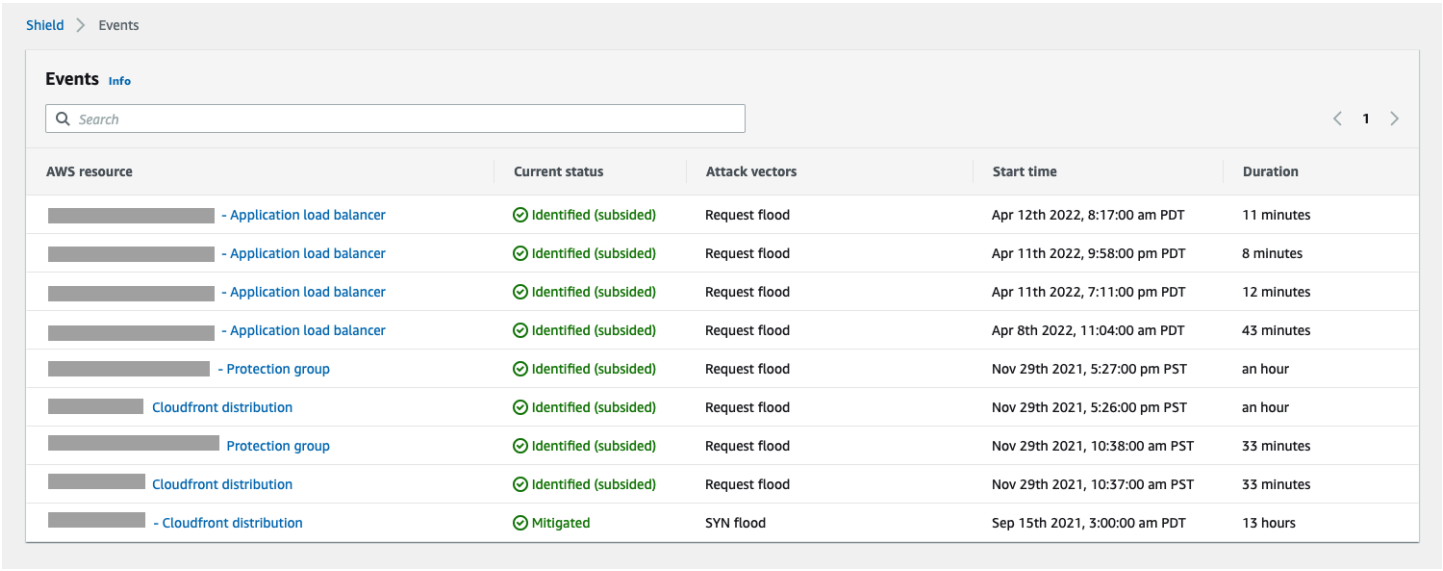
Vous pouvez accéder aux résumés et aux détails des événements via la page Événements de la console Shield. La page Événements de haut niveau fournit un aperçu des événements actuels et passés.

La capture d'écran suivante montre un exemple de page d'événements avec un seul événement en cours. Cet événement actif est également signalé dans le volet de navigation de gauche.



Shield Advanced peut également mettre en place automatiquement des mesures d'atténuation contre les attaques, en fonction du type de trafic et des protections que vous avez configurées. Ces mesures d'atténuation peuvent empêcher votre ressource de recevoir du trafic excessif ou du trafic correspondant à une signature d'attaque DDoS connue.

La capture d'écran suivante montre un exemple de liste d'événements dans lequel tous les événements ont été atténués par Shield Advanced ou se sont atténués d'eux-mêmes.



Protégez vos ressources avant un événement

Améliorez la précision de la détection des événements en protégeant les ressources avec Shield Advanced alors qu'elles reçoivent le trafic normal attendu, avant qu'elles ne soient soumises à une attaque DDoS.

Afin de signaler avec précision les événements relatifs à une ressource protégée, Shield Advanced doit d'abord établir une base de référence des modèles de trafic attendus pour cette ressource.

- Shield Advanced signale les événements liés à la couche d'infrastructure relatifs aux ressources après qu'elles ont été protégées pendant au moins 15 minutes.
- Shield Advanced signale les événements de la couche d'application Web pour les ressources après qu'elles ont été protégées pendant au moins 24 heures. La précision de détection des événements liés à la couche application est optimale une fois que Shield Advanced a observé le trafic attendu pendant 30 jours.

Pour accéder aux informations relatives aux événements dans la AWS Shield console

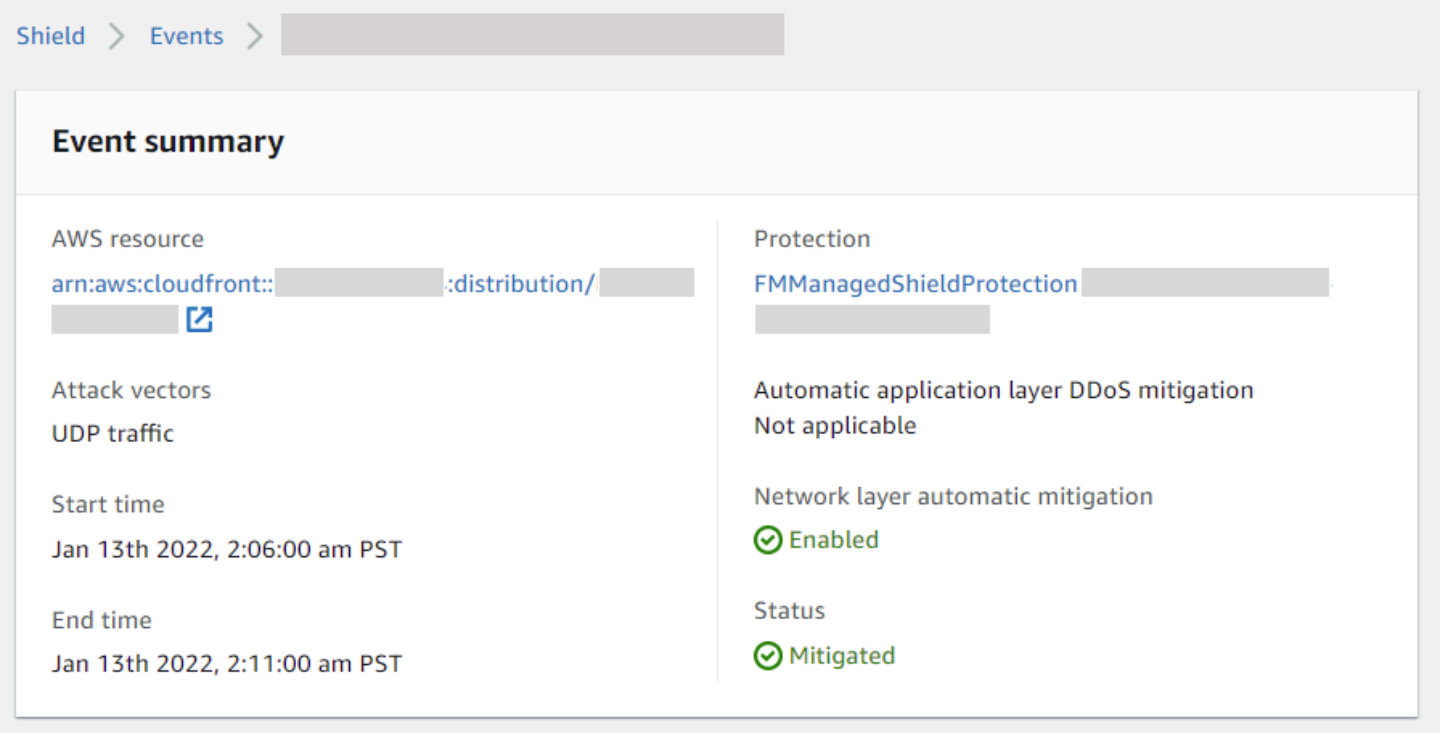
1. Connectez-vous à la console AWS WAF & Shield AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/wafv2/.
2. Dans le volet AWS Shield de navigation, sélectionnez Events. La console affiche la page Événements.
3. Sur la page Événements, vous pouvez sélectionner n'importe quel événement dans la liste pour voir des informations récapitulatives et des détails supplémentaires sur l'événement.

Rubriques

AWS Shield Advanced résumés des événements

Vous pouvez consulter le résumé et les informations détaillées d'un événement sur la page de console de l'événement. Pour ouvrir la page d'un événement, sélectionnez le nom de sa AWS ressource dans la liste des pages Événements.

La capture d'écran suivante montre un exemple de résumé d'événement pour un événement de couche réseau.



Les informations récapitulatives de la page de l'événement incluent les informations suivantes.

- État actuel : valeurs qui indiquent l'état de l'événement et les mesures prises par Shield Advanced pour y remédier. Les valeurs d'état s'appliquent aux événements de la couche infrastructure (couche 3 ou 4) et de la couche application (couche 7).
  - Identifié (en cours) et Identifié (diminué) : cela indique que Shield Advanced a détecté un événement, mais n'a pris aucune mesure pour y remédier jusqu'à présent. Identifié (diminué) indique que le trafic suspect détecté par Shield s'est arrêté sans intervention.
  - Atténuation en cours et atténuation : cela indique que Shield Advanced a détecté un événement et a pris des mesures pour y remédier. La méthode Mitiated est également utilisée lorsque la ressource ciblée est une CloudFront distribution Amazon ou une zone hébergée Amazon Route 53, qui disposent de leurs propres mesures d'atténuation automatiques intégrées.
- Vecteurs d'attaque : vecteurs d'attaque DDoS tels que TCP SYN flood et systèmes heuristiques de détection Shield Advanced tels que le flood de requêtes. Il peut s'agir d'indicateurs d'une attaque DDoS.
- Heure de début : date et heure auxquelles le premier point de données de trafic anormal a été détecté.

- Durée ou heure de fin : indique le temps écoulé entre l'heure de début de l'événement et le dernier point de données anormal observé par Shield Advanced. Pendant qu'un événement est en cours, ces valeurs continueront d'augmenter.
- Protection : nomme la protection Shield Advanced associée à la ressource et fournit un lien vers sa page de protection. Ceci est disponible sur la page de chaque événement.
- Atténuation automatique des attaques DDoS au niveau de la couche application : utilisée pour la protection de la couche application, pour indiquer si l'atténuation automatique des attaques DDoS au niveau de la couche application Shield Advanced est activée pour la ressource. S'il est activé, il fournit un lien permettant d'accéder à la configuration et de la gérer. Ceci est disponible sur la page de chaque événement.
- Atténuation automatique de la couche réseau : indique si la ressource dispose d'une atténuation automatique au niveau de la couche réseau. Si une ressource possède un composant de couche réseau, celui-ci sera activé. Ces informations sont disponibles sur la page de chaque événement.

Pour les ressources fréquemment ciblées, Shield peut laisser des mesures d'atténuation en place une fois que le trafic excédentaire aura diminué, afin d'éviter de nouveaux événements récurrents.

> **Note**
>
> Vous pouvez également accéder aux résumés des événements relatifs aux ressources protégées par le biais de l'opération AWS Shield ListAttacksAPI.

AWS Shield Advanced détails de l'événement

Vous pouvez consulter les détails relatifs à la détection, à l'atténuation et aux principaux contributeurs d'un événement dans la section inférieure de la page de console de l'événement. Cette section peut inclure un mélange de trafic légitime et potentiellement indésirable, et peut représenter à la fois le trafic transmis à votre ressource protégée et le trafic bloqué par les mesures d'atténuation du Shield.

- Détection et atténuation : fournit des informations sur l'événement observé et les mesures d'atténuation appliquées pour le contrer. Pour plus d'informations sur l'atténuation des événements, consultezRéagir aux événements DDoS.
- Principaux contributeurs : classe le trafic impliqué dans l'événement et répertorie les principales sources de trafic identifiées par Shield pour chaque catégorie. Pour les événements de la couche application, utilisez les informations des principaux contributeurs pour avoir une idée générale de

la nature d'un événement, mais utilisez les AWS WAF journaux pour vos décisions en matière de sécurité. Pour plus d'informations, consultez les sections suivantes.

Les informations relatives à vos événements dans la console Shield Advanced sont basées sur les métriques de Shield Advanced. Pour plus d'informations sur les métriques Shield Advanced, voir AWS Shield Advanced métriques

Les mesures d'atténuation ne sont pas incluses pour les ressources Amazon CloudFront ou Amazon Route 53, car ces services sont protégés par un système d'atténuation toujours activé et ne nécessitant pas de mesures d'atténuation pour les ressources individuelles.

Les sections détaillées varient selon que les informations concernent une couche d'infrastructure ou un événement de couche d'application.

Détails des événements de la couche d'application

Vous pouvez consulter les détails relatifs à la détection, à l'atténuation et aux principaux contributeurs d'un événement de couche application dans la section inférieure de la page de console de l'événement. Cette section peut inclure un mélange de trafic légitime et potentiellement indésirable, et peut représenter à la fois le trafic transmis à votre ressource protégée et le trafic bloqué par les mesures d'atténuation de Shield Advanced.

Les détails de l'atténuation concernent toutes les règles de l'ACL Web associées à la ressource, y compris les règles déployées spécifiquement en réponse à une attaque et les règles basées sur le taux définies dans l'ACL Web. Si vous activez l'atténuation automatique des attaques DDoS au niveau de la couche d'application pour une application, les mesures d'atténuation incluent des mesures pour ces règles supplémentaires. Pour plus d'informations sur ces protections de la couche d'application, consultezAWS Shield Advanced protections de la couche d'application (couche 7).

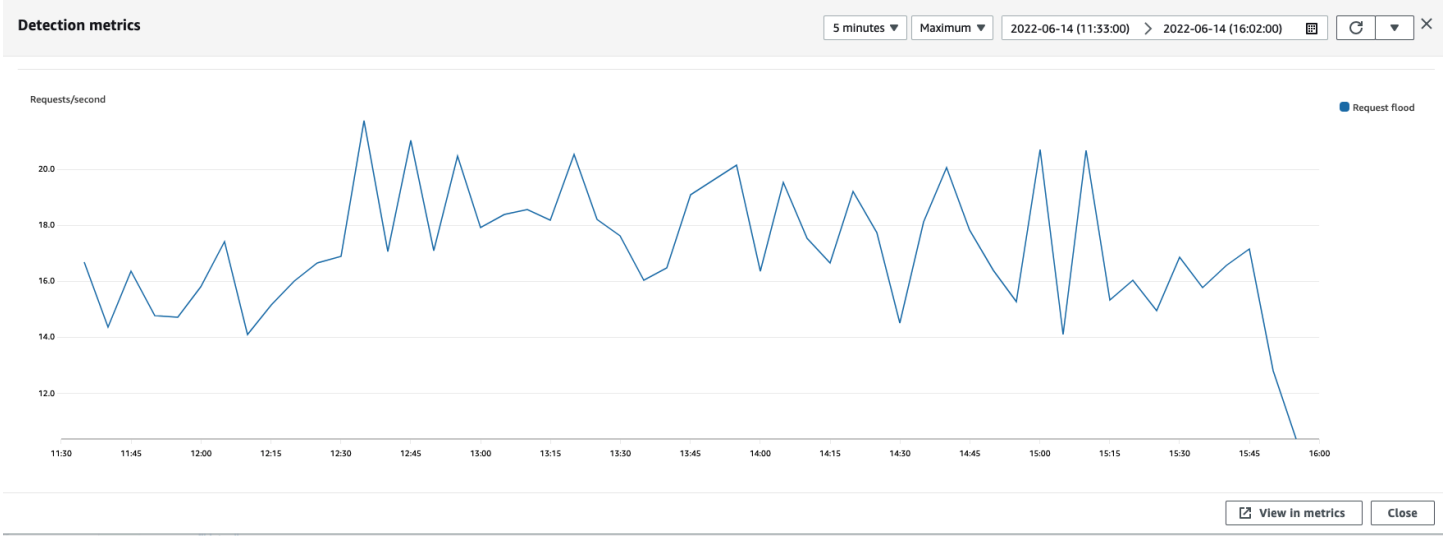
Détection et atténuation

Pour un événement de couche d'application (couche 7), l'onglet Détection et atténuation affiche les mesures de détection basées sur les informations obtenues à partir des AWS WAF journaux. Les mesures d'atténuation sont basées sur AWS WAF les règles de l'ACL Web associée qui sont configurées pour bloquer le trafic indésirable.

Pour les CloudFront distributions Amazon, vous pouvez configurer Shield Advanced pour appliquer des mesures d'atténuation automatiques à votre place. Quelles que soient les ressources de la couche application, vous pouvez choisir de définir vos propres règles d'atténuation dans votre ACL

Web et demander de l'aide à la Shield Response Team (SRT). Pour de plus amples informations sur ces options, consultez Réagir aux événements DDoS.

La capture d'écran suivante montre un exemple de mesures de détection pour un événement de couche application qui s'est atténué après un certain nombre d'heures.



Le trafic d'événements qui s'atténue avant l'entrée en vigueur d'une règle d'atténuation n'est pas représenté dans les mesures d'atténuation. Cela peut entraîner une différence entre le trafic de requêtes Web indiqué dans les graphiques de détection et les mesures d'autorisation et de blocage indiquées dans les graphiques d'atténuation.

Principaux contributeurs

L'onglet Principaux contributeurs pour les événements de la couche application affiche les 5 principaux contributeurs identifiés par Shield pour l'événement, sur la base AWS WAF des journaux qu'il a récupérés. Shield classe les informations des principaux contributeurs par des dimensions telles que l'adresse IP source, le pays source et l'URL de destination.

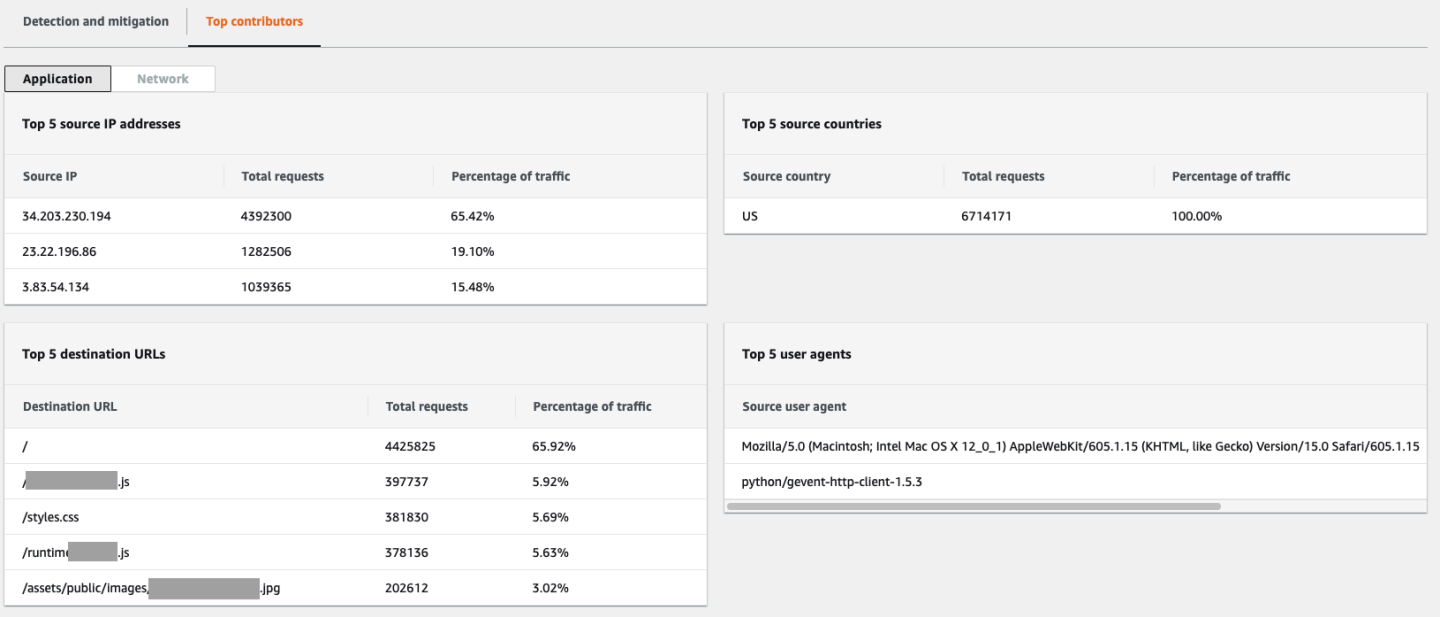
> **Note**
>
> Pour obtenir les informations les plus précises sur le trafic qui contribue à un événement de couche application, utilisez les AWS WAF journaux.

Utilisez les informations sur les principaux contributeurs de la couche d'application Shield uniquement pour avoir une idée générale de la nature d'une attaque, et ne basez pas vos décisions en matière de sécurité sur ces informations. En ce qui concerne les événements liés à la couche application, les

AWS WAF journaux constituent la meilleure source d'informations pour comprendre les facteurs à l'origine d'une attaque et pour concevoir vos stratégies d'atténuation.

Les informations sur les principaux contributeurs du Shield ne reflètent pas toujours complètement les données contenues dans les AWS WAF journaux. Lorsqu'il ingère les journaux, Shield donne la priorité à la réduction de l'impact sur les performances du système plutôt qu'à la récupération de l'ensemble complet des données des journaux. Cela peut entraîner une perte de granularité des données mises à la disposition de Shield pour analyse. Dans la plupart des cas, la majorité des informations sont disponibles, mais il est possible que les données des principaux contributeurs soient faussées dans une certaine mesure en cas d'attaque.

La capture d'écran suivante montre un exemple d'onglet Principaux contributeurs pour un événement de couche application.



Les informations des contributeurs sont basées sur les demandes de trafic légitime et potentiellement indésirable. Les événements de plus grand volume et les événements dont les sources de requêtes ne sont pas très distribuées sont plus susceptibles d'avoir des contributeurs de premier plan identifiables. Une attaque distribuée de manière significative peut avoir plusieurs sources, ce qui complique l'identification des principaux contributeurs à l'attaque. Si Shield Advanced n'identifie pas les contributeurs importants pour une catégorie spécifique, il affiche les données comme non disponibles.

Détails des événements relatifs à la couche d'infrastructure

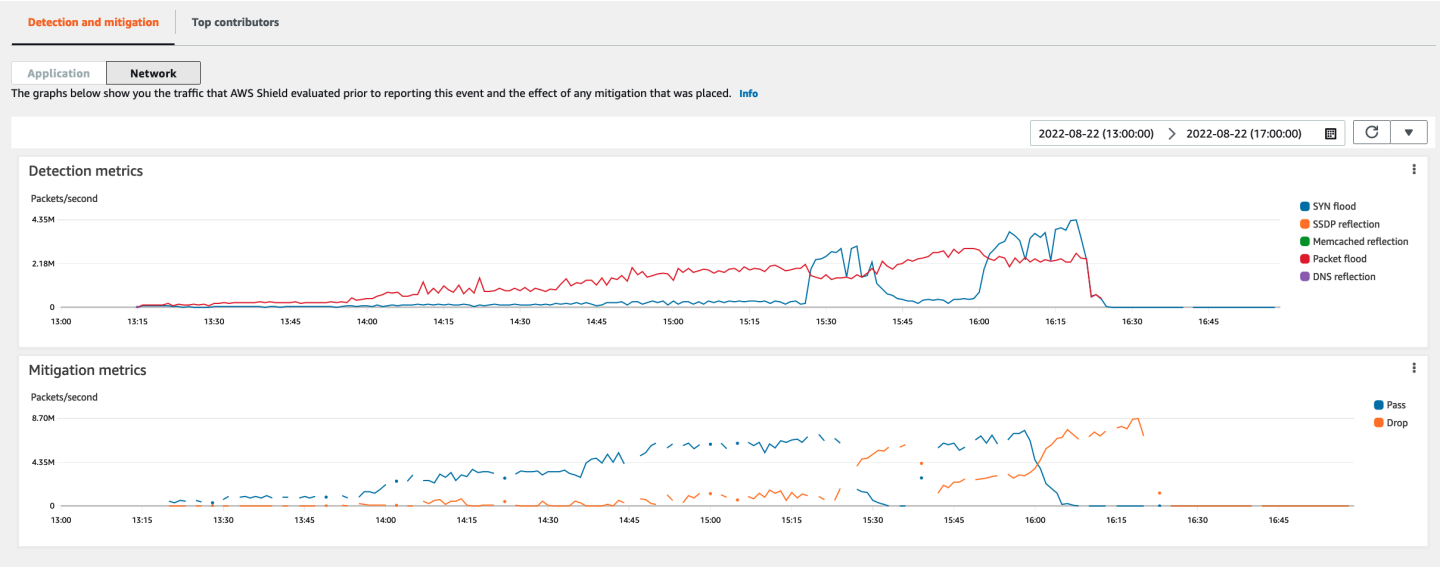
Vous pouvez consulter les détails relatifs à la détection, à l'atténuation et aux principaux contributeurs d'un événement au niveau de la couche d'infrastructure dans la section inférieure de la page de console de l'événement. Cette section peut inclure un mélange de trafic légitime et potentiellement indésirable, et peut représenter à la fois le trafic transmis à votre ressource protégée et le trafic bloqué par les mesures d'atténuation du Shield.

Détection et atténuation

Pour un événement de couche d'infrastructure (couche 3 ou 4), l'onglet Détection et atténuation affiche les mesures de détection basées sur des flux réseau échantillonnés et les mesures d'atténuation basées sur le trafic observé par les systèmes d'atténuation. Les mesures d'atténuation sont une mesure plus précise du trafic vers votre ressource.

Shield crée automatiquement une atténuation pour les types de ressources protégés Elastic IP (EIP), Classic Load Balancer (CLB), Application Load Balancer (ALB) et accélérateur standard. AWS Global Accelerator Les mesures d'atténuation pour les adresses EIP et les accélérateurs AWS Global Accelerator standard indiquent le nombre de paquets transmis et abandonnés.

La capture d'écran suivante montre un exemple d'onglet Détection et atténuation pour un événement de couche d'infrastructure.

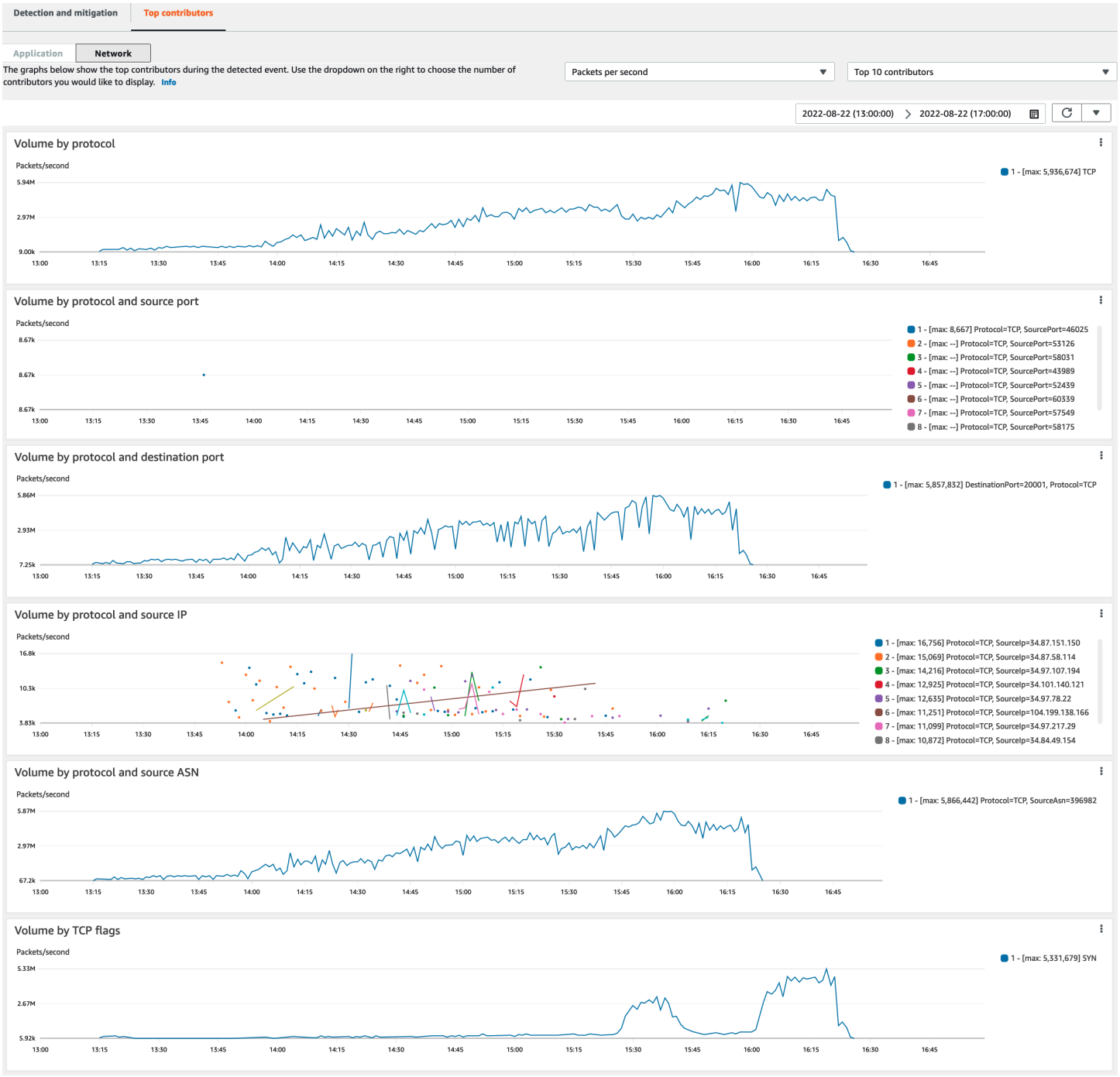


Le trafic d'événements qui s'atténue avant que Shield ne mette en place une mesure d'atténuation n'est pas représenté dans les mesures d'atténuation. Cela peut entraîner une différence entre le trafic indiqué dans les graphiques de détection et les mesures de réussite et de baisse indiquées dans les graphiques d'atténuation.

Principaux contributeurs

L'onglet Principaux contributeurs pour les événements de la couche infrastructure répertorie les mesures relatives à un maximum de 100 principaux contributeurs sur plusieurs dimensions du trafic. Les détails incluent les propriétés de la couche réseau pour toutes les dimensions dans lesquelles au moins cinq sources importantes de trafic peuvent être identifiées. L'adresse IP source et l'ASN source sont des exemples de sources de trafic.

La capture d'écran suivante montre un exemple d'onglet Principaux contributeurs pour un événement de couche d'infrastructure.



Les indicateurs des contributeurs sont basés sur des échantillons de flux réseau pour le trafic légitime et potentiellement indésirable. Les événements de plus grand volume et les événements dont les sources de trafic ne sont pas très distribuées sont plus susceptibles d'avoir des contributeurs de premier plan identifiables. Une attaque distribuée de manière significative peut avoir plusieurs sources, ce qui complique l'identification des principaux contributeurs à l'attaque. Si Shield n'identifie aucun contributeur significatif pour une métrique ou une catégorie spécifique, il affiche les données comme non disponibles.

Lors d'une attaque DDoS au niveau de l'infrastructure, les sources de trafic peuvent être falsifiées ou reflétées. Une source falsifiée est forgée intentionnellement par l'attaquant. Une source réfléchie est la véritable source du trafic détecté, mais elle ne participe pas volontairement à l'attaque. Par exemple, un attaquant peut générer un flux important et amplifié de trafic vers une cible en reflétant l'attaque dirigée contre des services sur Internet qui sont généralement légitimes. Dans ce cas, les informations de source peuvent être valides alors qu'elles ne sont pas la véritable source de l'attaque. Ces facteurs peuvent limiter la viabilité des techniques d'atténuation qui bloquent les sources en fonction des en-têtes de paquets.

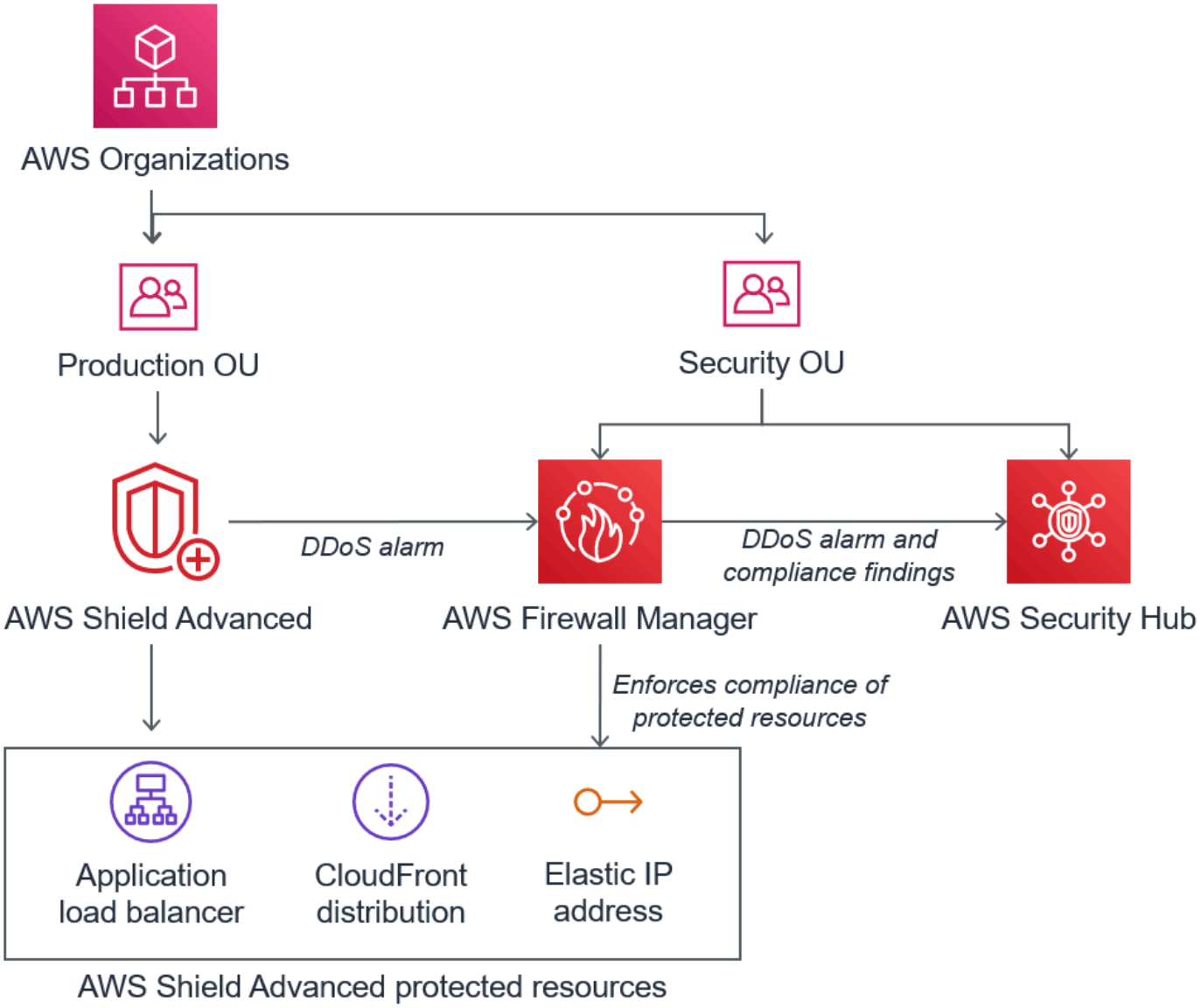
Visibilité des événements sur tous les comptes

Vous pouvez utiliser, AWS Security Hub gérer AWS Firewall Manager et surveiller les ressources AWS Shield Advanced protégées sur plusieurs comptes.

Avec Firewall Manager, vous pouvez créer une politique de sécurité Shield Advanced qui signale et applique la conformité en matière de protection contre les attaques DDoS sur l'ensemble de vos comptes. Firewall Manager surveille vos ressources protégées, notamment en ajoutant des protections aux nouvelles ressources couvertes par la politique Shield Advanced.

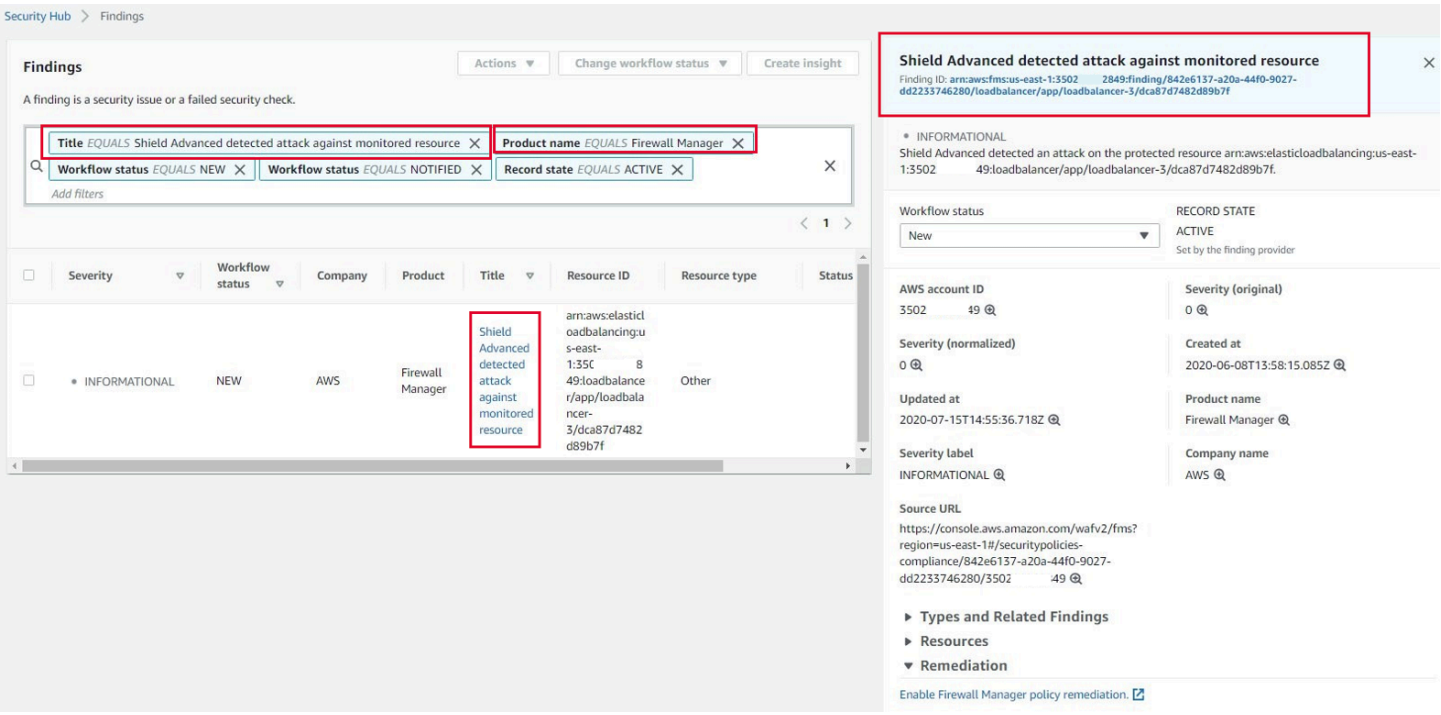
Vous pouvez intégrer Firewall Manager AWS Security Hub pour obtenir un tableau de bord unique signalant les événements DDoS détectés par Shield Advanced et les résultats de conformité de Firewall Manager, lorsque Firewall Manager identifie une ressource non conforme à votre politique de sécurité Shield Advanced.

La figure suivante décrit une architecture typique de surveillance des ressources protégées de Shield Advanced avec Firewall Manager et Security Hub.



Lorsque vous intégrez Firewall Manager à Security Hub, vous pouvez consulter les résultats de sécurité en un seul endroit, ainsi que les autres alertes et les informations sur le statut de conformité des applications sur lesquelles vous les exécutez AWS.

La capture d'écran suivante met en évidence les informations que vous pouvez voir concernant un événement Shield Advanced dans la console Security Hub lorsque vous disposez d'une intégration de ce type.



Pour savoir comment intégrer Firewall Manager et Security Hub à Shield Advanced afin de centraliser la surveillance des événements et de la conformité sur vos comptes protégés, consultez le blog sur la AWS sécurité Configurer une surveillance centralisée des événements DDoS et corriger automatiquement les ressources non conformes.

Réagir aux événements DDoS

AWS atténue automatiquement les attaques par déni de service distribué (DDoS) du réseau et des couches de transport (couches 3 et 4). Si vous utilisez Shield Advanced pour protéger vos instances Amazon EC2, lors d'une attaque, Shield Advanced déploie automatiquement les ACL de votre réseau Amazon VPC à la limite du réseau. AWS Cela permet à Shield Advanced de fournir une protection contre les événements DDoS plus importants. Pour plus d'informations sur les listes ACL réseau, consultez Listes ACL réseau.

Pour les attaques DDoS au niveau de l'application (couche 7), AWS tentatives de détection et de notification des AWS Shield Advanced clients par le biais d' CloudWatch alarmes. Par défaut, il n'applique pas automatiquement les mesures d'atténuation, afin d'éviter de bloquer par inadvertance le trafic utilisateur valide.

Pour les ressources de la couche application (couche 7), les options suivantes sont disponibles pour répondre à une attaque.

- Proposez vos propres mesures d'atténuation — Vous pouvez étudier et atténuer vous-même l'attaque. Pour plus d'informations, consultez Atténuation manuelle d'une attaque DDoS au niveau de la couche applicative.
- Contacter l'assistance — Si vous êtes un client de Shield Advanced, vous pouvez contacter le AWS Support Centre pour obtenir de l'aide concernant les mesures d'atténuation. Les cas critiques et urgents sont acheminés directement vers des experts DDoS. Pour plus d'informations, consultez Contacter le centre de support lors d'une attaque DDoS au niveau de la couche applicative.

En outre, avant qu'une attaque ne se produise, vous pouvez activer de manière proactive les options d'atténuation suivantes :

- Atténuations automatiques sur les CloudFront distributions Amazon : avec cette option, Shield Advanced définit et gère les règles d'atténuation pour vous dans votre ACL Web. Pour plus d'informations sur l'atténuation automatique de la couche d'application, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.
- Engagement proactif : lorsqu'il AWS Shield Advanced détecte une attaque de grande envergure contre l'une de vos applications, le SRT peut vous contacter de manière proactive. Le SRT trie l'événement DDoS et crée des mesures d'atténuation. AWS WAF La SRT vous contacte et, avec votre accord, peut appliquer les AWS WAF règles. Pour plus d'informations sur cette option, consultez Configuration de l'engagement proactif.

Contacter le centre de support lors d'une attaque DDoS au niveau de la couche applicative

Si vous êtes AWS Shield Advanced client, vous pouvez contacter le AWS Support Centre pour obtenir de l'aide concernant les mesures d'atténuation. Les cas critiques et urgents sont acheminés directement vers des experts DDoS. Les cas complexes peuvent ainsi être transmis à la AWS Shield Response Team (SRT), qui possède une vaste expérience dans le domaine de la protection AWS d'Amazon.com et de ses filiales. AWS Shield Advanced Pour plus d'informations sur le SRT, consultezAssistance de la Shield Response Team (SRT).

Pour obtenir l'assistance de la Shield Response Team (SRT), contactez le AWS Support Center. Le temps de réponse de votre dossier dépend de la gravité que vous sélectionnez et des temps de réponse, qui sont documentés sur la page AWS Support Plans.

Sélectionnez les options suivantes :

- Type de cas : Support technique
- Service : DDoS (Distributed Denial of Service)
- Catégorie : Entrant vers AWS
- Gravité : Choisissez une action appropriée

Lorsque vous discutez avec notre représentant, expliquez que vous êtes un AWS Shield Advanced client victime d'une éventuelle attaque DDoS. Notre représentant dirigera votre appel vers les experts DDoS appropriés. Si vous ouvrez un dossier auprès du AWS Support Centre en utilisant le type de service de déni de service distribué (DDoS), vous pouvez parler directement à un expert DDoS par chat ou par téléphone. Les ingénieurs du support DDoS peuvent vous aider à identifier les attaques, à recommander des améliorations à apporter à votre AWS architecture et à vous conseiller sur l'utilisation des AWS services destinés à atténuer les attaques DDoS.

Pour les attaques de la couche applicative, le SRT peut vous aider à analyser les activités suspectes. Si l'atténuation automatique est activée pour votre ressource, le SRT peut examiner les mesures d'atténuation que Shield Advanced place automatiquement contre l'attaque. Dans tous les cas, le SRT peut vous aider à examiner et à atténuer le problème. Les mesures d'atténuation recommandées par le SRT nécessitent souvent que le SRT crée ou mette à jour des listes de contrôle d'accès AWS WAF Web (ACL Web) dans votre compte. Le SRT aura besoin de votre autorisation pour effectuer ce travail.

> **Important**
>
> Dans le cadre de l'activation AWS Shield Advanced, nous vous recommandons de suivre les étapes ci-dessous Configuration de l'accès pour la Shield Response Team (SRT) pour fournir de manière proactive au SRT les autorisations dont il a besoin pour vous aider lors d'une attaque. La fourniture préalable de l'autorisation permet d'éviter tout retard en cas d'attaque réelle.

Le SRT vous aide à trier les attaques DDoS afin d'identifier les signatures et les modèles d'attaque. Avec votre accord, le SRT crée et déploie des AWS WAF règles pour atténuer l'attaque.

Vous pouvez également contacter le SRT avant ou pendant une éventuelle attaque pour examiner les mesures d'atténuation et pour développer et déployer des mesures d'atténuation personnalisées. Par exemple, si vous exécutez une application Web et que seuls les ports 80 et 443 sont ouverts,

vous pouvez utiliser le SRT pour préconfigurer une ACL Web afin d' « autoriser » uniquement les ports 80 et 443.

Vous autorisez et contactez le SRT au niveau du compte. En d'autres termes, si vous utilisez Shield Advanced dans le cadre d'une politique de Firewall Manager Shield Advanced, c'est le propriétaire du compte, et non l'administrateur de Firewall Manager, qui doit contacter le SRT pour obtenir de l'aide. L'administrateur de Firewall Manager ne peut contacter le SRT que pour les comptes qu'il possède.

Atténuation manuelle d'une attaque DDoS au niveau de la couche applicative

Si vous déterminez que l'activité de la page des événements de votre ressource représente une attaque DDoS, vous pouvez créer vos propres AWS WAF règles dans votre ACL Web pour atténuer l'attaque. C'est la seule option disponible si vous n'êtes pas client de Shield Advanced. AWS WAF est inclus sans AWS Shield Advanced frais supplémentaires. Pour plus d'informations sur la création de règles dans votre ACL Web, consultezAWS WAF listes de contrôle d'accès Web (ACL Web).

Si vous l'utilisez AWS Firewall Manager, vous pouvez ajouter vos AWS WAF règles à une AWS WAF politique de Firewall Manager.

Pour atténuer manuellement une attaque DDoS potentielle au niveau de la couche applicative

1. Créez des instructions de règles dans votre ACL Web avec des critères correspondant au comportement inhabituel. Pour commencer, configurez-les pour compter les demandes correspondantes. Pour plus d'informations sur la configuration de votre ACL Web et de vos instructions de règles, consultez Évaluation des règles ACL Web et des groupes de règles etTester et ajuster vos AWS WAF protections.

   > **Note**
   >
   > Testez toujours vos règles d'abord en utilisant initialement l'action de la règle Count au lieu deBlock. Une fois que vous êtes certain que vos nouvelles règles identifient les bonnes demandes, vous pouvez les modifier pour bloquer les demandes.

2. Surveillez le nombre de demandes pour déterminer si vous souhaitez bloquer les demandes correspondantes. Si le volume de demandes continue d'être anormalement élevé et que vous êtes certain que vos règles tiennent compte des demandes à l'origine de ce volume élevé, modifiez les règles de votre ACL Web pour bloquer les demandes.

3. Continuez à surveiller la page des événements pour vous assurer que votre trafic est traité comme vous le souhaitez.

AWS fournit des modèles préconfigurés pour vous aider à démarrer rapidement. Les modèles incluent un ensemble de AWS WAF règles que vous pouvez personnaliser et utiliser pour bloquer les attaques Web courantes. Pour plus d'informations, consultez le document sur les automatisations de sécuritéAWS WAF.

Demande de crédit en AWS Shield Advanced

Si vous êtes abonné AWS Shield Advanced et que vous êtes victime d'une attaque DDoS qui augmente l'utilisation d'une ressource protégée par Shield Advanced, vous pouvez demander un crédit de service Shield Advanced pour les frais liés à cette utilisation accrue, dans la mesure où elle n'est pas atténuée par Shield Advanced.

> **Note**
>
> Vous ne pouvez appliquer les crédits reçus dans le cadre de ce processus qu'à l'utilisation de Shield Advanced. Les crédits Shield Advanced ne peuvent pas être utilisés avec d'autres services.

Les crédits ne sont disponibles que pour les types de frais suivants :

- Transfert de données Shield Advanced
- Requêtes CloudFront HTTP/HTTPS d'Amazon
- CloudFront transfert de données sortantes
- Requêtes Amazon Route 53
- AWS Global Accelerator transfert de données par accélérateur standard
- Unités de capacité d'équilibrage de charge pour Application Load Balancer
- Coûts d'instance pour les instances Amazon Elastic Compute Cloud (Amazon EC2) protégées créées par une politique d'auto-scaling en réponse à l'attaque

Conditions préalables à la demande de crédit

Pour être éligible à recevoir un crédit, avant le début de l'attaque, vous devez avoir effectué les opérations suivantes :

- Vous devez avoir ajouté la protection Shield Advanced aux ressources pour lesquelles vous souhaitez demander un crédit. Les ressources protégées ajoutées lors d'une attaque ne sont pas éligibles à la protection des coûts.

  > **Note**
  >
  > L'activation de Shield Advanced sur votre Compte AWS ordinateur n'active pas automatiquement la protection Shield Advanced pour les ressources individuelles.

  Pour plus d'informations sur la façon de protéger les AWS ressources à l'aide de Shield Advanced, consultezAjouter AWS Shield Advanced une protection aux AWS ressources.
- Pour les ressources applicables CloudFront et protégées par Application Load Balancer, vous devez avoir associé une ACL AWS WAF Web et implémenté une règle basée sur le taux dans l'ACL Web en mode. Block Pour plus d'informations sur les règles AWS WAF basées sur les taux, consultezInstruction de règle basée sur un taux. Pour plus d'informations sur la façon d'associer des ACL Web à des AWS ressources, consultezAWS WAF listes de contrôle d'accès Web (ACL Web).
- Vous devez avoir mis en œuvre les meilleures pratiques appropriées dans AWS Best Practices for DDoS Resiliency afin de configurer votre application de manière à minimiser les coûts lors d'une attaque DDoS.

Comment faire une demande de crédit

Pour être éligible à un crédit, vous devez soumettre votre demande de crédit dans les 15 jours suivant immédiatement le mois de facturation au cours duquel l'attaque s'est produite.

Pour demander un crédit, soumettez un dossier de facturation par l'intermédiaire du AWS Support Centre. Incluez les éléments suivants dans votre demande :

- La mention « DDoS Concession » dans la ligne d'objet
- Les dates et heures de chaque événement ou interruption de disponibilité pour lequel vous demandez un crédit
- Les AWS services et les ressources spécifiques concernés

Après avoir soumis une demande, la AWS Shield Response Team (SRT) validera si une attaque DDoS s'est produite et, dans l'affirmative, si des ressources protégées ont été redimensionnées pour absorber l'attaque DDoS. S'il est AWS déterminé que les ressources protégées ont été dimensionnées pour absorber l'attaque DDoS, il AWS émettra un crédit pour la partie du trafic qui a été AWS déterminée par l'attaque DDoS. Les crédits sont valides pendant 12 mois.

Sécurité lors de votre utilisation du AWS Shield service

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

> **Note**
>
> Cette section fournit des conseils AWS de sécurité standard pour votre utilisation du AWS Shield service et de ses AWS ressources, telles que les protections Shield Advanced. Pour plus d'informations sur la protection de vos AWS ressources à l'aide de Shield et Shield Advanced, consultez le reste du AWS Shield guide.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. L'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Shield, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation ainsi que les lois et réglementations applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Shield. Les rubriques suivantes expliquent comment configurer Shield pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources du Shield.

Rubriques

Protection des données dans Shield

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Shield. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu’Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.

- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Shield ou un autre utilisateur Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Les entités du Shield, telles que les protections, sont cryptées au repos, sauf dans certaines régions où le chiffrement n'est pas disponible, notamment en Chine (Pékin) et en Chine (Ningxia). Des clés de chiffrement uniques sont utilisées pour chaque région.

Gestion des identités et des accès pour AWS Shield

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources du Shield. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Shield.

Utilisateur du service : si vous utilisez le service Shield pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités du Shield pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans Shield, consultezRésolution des problèmes AWS Shield d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des ressources du Shield au sein de votre entreprise, vous avez probablement un accès complet à Shield. C'est à vous de déterminer les fonctionnalités et les ressources du Shield auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM with Shield, consultezComment AWS Shield fonctionne avec IAM.

Administrateur IAM — Si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Shield. Pour consulter des exemples de politiques basées sur l'identité du Shield que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour AWS Shield

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur

qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console

changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer

d’autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d’accès.

- Rôle de service : il s’agit d’un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d’IAM. Pour plus d’informations, consultez Création d’un rôle pour la délégation d’autorisations à un Service AWS dans le Guide de l’utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d’effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d’accès au sein de l’instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d’instance contient le rôle et permet aux programmes qui s’exécutent sur l’instance EC2 d’obtenir des informations d’identification temporaires. Pour plus d’informations, consultez Utilisation d’un rôle IAM pour accorder des autorisations à des applications s’exécutant sur des instances Amazon EC2 dans le Guide de l’utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d’un utilisateur) dans le Guide de l’utilisateur IAM.

Gestion des accès à l’aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d’informations sur la structure et le contenu des documents de politique JSON, consultez Vue d’ensemble des politiques JSON dans le Guide de l’utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les

ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités

figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .

- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS Shield fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Shield, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Shield.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Shield

Fonction IAM	Support Shield
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui

Fonction IAM	Support Shield
ACL	Non
ABAC (identifications dans les politiques)	Partielle
Informations d’identification temporaires	Oui
Transmission des sessions d’accès (FAS)	Oui
Fonctions de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont Shield et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez la section AWS Services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Shield

Prend en charge les politiques basées sur l’identité	Oui

Les politiques basées sur l’identité sont des documents de politique d’autorisations JSON que vous pouvez attacher à une identité telle qu’un utilisateur, un groupe d’utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d’actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l’identité, consultez Création de politiques IAM dans le Guide de l’utilisateur IAM.

Avec les politiques IAM basées sur l’identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s’applique à l’utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l’utilisateur IAM.

Pour consulter des exemples de politiques basées sur l'identité du Shield, consultez. Exemples de politiques basées sur l’identité pour AWS Shield

Politiques basées sur les ressources au sein de Shield

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions politiques pour Shield

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom

que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions du Shield, consultez la section Actions définies par AWS Shield dans le Service Authorization Reference.

Les actions politiques dans Shield utilisent le préfixe suivant avant l'action :

```
shield
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "shield:action1",
      "shield:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions commençant par « Shield »`List`, incluez l'action suivante :

```
"Action": "shield:List*"
```

Pour consulter des exemples de politiques basées sur l'identité du Shield, consultez. Exemples de politiques basées sur l'identité pour AWS Shield

Ressources relatives aux politiques pour Shield

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources du Shield et de leurs ARN, consultez la section Ressources définies par AWS Shield dans le Service Authorization Reference. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Shield. Pour autoriser ou refuser l'accès à un sous-ensemble de ressources du Shield, incluez l'ARN de la ressource dans l'`resource`élément de votre politique.

Dans AWS Shield, les ressources sont les protections et les attaques. Ces ressources ont des noms ARN (Amazon Resource Name) uniques qui leur sont associés, comme cela est illustré dans le tableau suivant.

Nom dans la AWS Shield console	Nom dans le AWS Shield SDK/CLI	Format ARN
Événement ou attaque	`AttackDetail`	`arn:aws:shield:: account:attack/ID`
Protection	`Protection`	`arn:aws:shield:: account:protection/ ID`

Pour autoriser ou refuser l'accès à un sous-ensemble de ressources du Shield, incluez l'ARN de la ressource dans l'`resource`élément de votre politique. Les ARN de Shield ont le format suivant :

```
arn:partition:shield::account:resource/ID
```

Remplacez les variables *compte*, *ressources* et *ID* variables par des valeurs valides. Les valeurs valides peuvent être les suivantes :

- *compte* : L'identifiant de votre Compte AWS. Vous devez spécifier une valeur.
- *ressource* : le type de ressource Shield, `attack` soit`protection`.
- *ID* : ID de la ressource Shield, ou un caractère générique (*) pour indiquer toutes les ressources du type spécifié associées à la ressource spécifiée Compte AWS.

Par exemple, l'ARN suivante spécifie toutes les protections pour le compte `111122223333` :

```
arn:aws:shield::111122223333:protection/*
```

Les ressources ARNs of Shield ont le format suivant :

```
arn:partition:shield:region:account-id:scope/resource-type/resource-name/resource-id
```

Pour obtenir des informations générales sur les spécifications des ARN, consultez Amazon Resource Names (ARN) dans le Référence générale d'Amazon Web Services.

La liste suivante répertorie les exigences spécifiques aux ARN des `wafv2` ressources :

- *région* : pour les ressources Shield que vous utilisez pour protéger les CloudFront distributions Amazon, définissez cette option sur`us-east-1`. Sinon, définissez ce paramètre sur la région que vous utilisez avec vos ressources régionales protégées.
- *portée* : définissez le champ d'application `global` pour une utilisation avec une CloudFront distribution Amazon ou `regional` pour une utilisation avec l'une des ressources régionales prises AWS WAF en charge. Les ressources régionales sont une API REST Amazon API Gateway, un Application Load Balancer, une API AWS AppSync GraphQL, un groupe d'utilisateurs Amazon Cognito, un AWS App Runner service et une instance Verified Access. AWS
- *resource-type* : Spécifiez l'une des valeurs suivantes : `attack` pour les événements ou les attaques, `protection` pour les protections.
- *resource-name* : Spécifiez le nom que vous avez donné à la ressource Shield, ou spécifiez un caractère générique (*) pour indiquer toutes les ressources qui répondent aux autres spécifications de l'ARN. Vous devez soit spécifier le nom et l'ID de la ressource, soit spécifier un caractère générique pour les deux.

- *resource-id* : Spécifiez l'ID de la ressource Shield ou spécifiez un caractère générique (*) pour indiquer toutes les ressources qui répondent aux autres spécifications de l'ARN. Vous devez soit spécifier le nom et l'ID de la ressource, soit spécifier un caractère générique pour les deux.

Par exemple, l'ARN suivante spécifie toutes les listes ACL web avec une portée régionale pour le compte 111122223333 dans la région us-west-1 :

```
arn:aws:wafv2:us-west-1:111122223333:regional/webacl/*/*
```

L'ARN suivant spécifie le groupe de règles nommé MyIPManagementRuleGroup avec une portée globale pour le compte 111122223333 dans Region us-east-1 :

```
arn:aws:wafv2:us-east-1:111122223333:global/rulegroup/MyIPManagementRuleGroup/1111aaaa-bbbb-cccc-dddd-example-id
```

Pour consulter des exemples de politiques basées sur l'identité du Shield, consultez. Exemples de politiques basées sur l’identité pour AWS Shield

Clés relatives aux conditions de politique pour Shield

Prend en charge les clés de condition de politique spécifiques au service	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C’est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L’élément Condition (ou le bloc Condition) vous permet de spécifier des conditions lorsqu’une instruction est appliquée. L’élément Condition est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments Condition dans une instruction, ou plusieurs clés dans un seul élément Condition, AWS les évalue à l’aide d’une opération AND logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une OR opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l’instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition du Shield, reportez-vous à la section Clés de condition correspondantes AWS Shield dans le Service Authorization Reference. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Shield.

Pour consulter des exemples de politiques basées sur l'identité du Shield, consultez. Exemples de politiques basées sur l'identité pour AWS Shield

ACL dans Shield

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Shield

Prise en charge d'ABAC (identifications dans les politiques)	Partielle

Le contrôle d'accès basé sur les attributs (ABAC) est une politique d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Shield

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires

au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Sessions d'accès transmises pour Shield

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Shield

Prend en charge les fonctions du service	Oui

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités du Shield. Modifiez les rôles de service uniquement lorsque Shield fournit des instructions à cet effet.

Rôles liés à un service pour Shield

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés aux services Shield, consultez. Utilisation de rôles liés à un service pour Shield Advanced

Exemples de politiques basées sur l'identité pour AWS Shield

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources du Shield. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM doit créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Shield, y compris le format des ARN pour chacun des types de ressources, voir Actions, ressources et clés de condition AWS Shield dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Shield
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Accordez un accès en lecture à vos protections Shield Advanced
- Accordez un accès en lecture seule à Shield, et CloudFront CloudWatch
- Accordez un accès complet à Shield CloudFront, et CloudWatch

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer les ressources du Shield dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour de plus amples informations, consultez Politiques gérées AWS ou Politiques gérées AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège - Lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez Politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès - Vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles - IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour de plus amples informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue.

Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour de plus amples informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Shield

Pour accéder à la AWS Shield console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les informations relatives aux ressources du Shield présentes dans votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Les utilisateurs autorisés à accéder à la AWS console et à l'utiliser peuvent également accéder à AWS Shield celle-ci. Aucune autorisation supplémentaire n'est requise.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
```

```
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accordez un accès en lecture à vos protections Shield Advanced

AWS Shield autorise l'accès aux ressources entre comptes, mais ne vous permet pas de créer des protections des ressources entre comptes. Vous pouvez uniquement créer des protections pour les ressources à partir du compte propriétaire de ces ressources.

Voici un exemple de stratégie qui accorde les autorisations requises pour l'action `shield:ListProtections` au niveau de toutes les ressources. Shield ne prend pas en charge l'identification de ressources spécifiques à l'aide des ARN des ressources (également appelées autorisations au niveau des ressources) pour certaines actions d'API. Vous devez donc spécifier un caractère générique (*). Cela permet uniquement d'accéder aux ressources que vous pouvez récupérer par le biais de l'action`ListProtections`.

```
{
    "Version": "2016-06-02",
    "Statement": [
        {
            "Sid": "ListProtections",
            "Effect": "Allow",
            "Action": [
```

```
                "shield:ListProtections"
            ],
            "Resource": "*"
        }
    ]
}
```

Accordez un accès en lecture seule à Shield, et CloudFront CloudWatch

La politique suivante accorde aux utilisateurs un accès en lecture seule à Shield et aux ressources associées, y compris les CloudFront ressources Amazon et les métriques Amazon CloudWatch . Il est utile pour les utilisateurs qui ont besoin d'une autorisation pour consulter les paramètres des protections et des attaques du Shield et pour surveiller les indicateurs dans CloudWatch. Ces utilisateurs ne peuvent pas créer, mettre à jour ou supprimer les ressources du Shield.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
                    "arn:aws:route53:::hostedzone/*",
                    "arn:aws:cloudwatch:*:*:*:*",
                    "arn:aws:globalaccelerator::*:*"
                ]
            },
```

```
            {
                "Sid": "ShieldReadOnly",
                "Effect": "Allow",
                "Action": [
                    "shield:List*",
                    "shield:Describe*",
                    "shield:Get*"
                ],
                "Resource": "*"
            }
    ]
}
```

Accordez un accès complet à Shield CloudFront, et CloudWatch

La politique suivante permet aux utilisateurs d'effectuer n'importe quelle opération du Shield, d'effectuer n'importe quelle opération sur les distributions CloudFront Web et de surveiller les métriques et un échantillon de requêtes introduites CloudWatch. C'est utile pour les utilisateurs qui sont administrateurs du Shield.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "ProtectedResourcesReadAccess",
                "Effect": "Allow",
                "Action": [
                    "cloudfront:List*",
                    "elasticloadbalancing:List*",
                    "route53:List*",
                    "cloudfront:Describe*",
                    "elasticloadbalancing:Describe*",
                    "route53:Describe*",
                    "cloudwatch:Describe*",
                    "cloudwatch:Get*",
                    "cloudwatch:List*",
                    "cloudfront:GetDistribution*",
                    "globalaccelerator:ListAccelerators",
                    "globalaccelerator:DescribeAccelerator"
                ],
                "Resource": [
                    "arn:aws:elasticloadbalancing:*:*:*",
                    "arn:aws:cloudfront::*:*",
```

```
                "arn:aws:route53:::hostedzone/*",
                "arn:aws:cloudwatch:*:*:*:*",
                "arn:aws:globalaccelerator::*:*"
            ]
        },
        {
            "Sid": "ShieldFullAccess",
            "Effect": "Allow",
            "Action": [
                "shield:*"
            ],
            "Resource": "*"
        }
    ]
}
```

Nous vous recommandons vivement de configurer Multi-Factor Authentication (MFA) pour les utilisateurs qui ont des autorisations d'administration. Pour plus d'informations, consultez la section Using Multi-Factor Authentication (MFA) Devices AWS with dans le guide de l'utilisateur IAM.

AWS politiques gérées pour AWS Shield

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : AWSShieldDRTAccessPolicy

AWS Shield utilise cette politique gérée lorsque vous autorisez la Shield Response Team (SRT) à agir en votre nom. Cette politique donne à la SRT un accès limité à votre AWS compte, afin de contribuer à atténuer les attaques DDoS lors d'événements très graves. Cette politique permet à la SRT de gérer vos AWS WAF règles et les protections de Shield Advanced et d'accéder à vos AWS WAF journaux.

Pour plus d'informations sur l'autorisation à la SRT d'opérer en votre nom, consultezConfiguration de l'accès pour la Shield Response Team (SRT).

Pour plus de détails sur cette politique, consultez AWSShieldDRTAccessPolicyla console IAM.

AWS politique gérée : AWSShieldServiceRolePolicy

Shield Advanced utilise cette politique gérée lorsque vous activez l'atténuation automatique des attaques DDoS au niveau de l'application, afin de définir les autorisations nécessaires pour gérer les ressources de votre compte. Cette politique permet à Shield Advanced de créer et d'appliquer des AWS WAF règles et des groupes de règles dans les ACL Web que vous avez associées à vos ressources protégées, afin de répondre automatiquement aux attaques DDoS.

Vous ne pouvez pas vous associer AWSShieldServiceRolePolicy à vos entités IAM. Shield associe cette politique au rôle lié au service afin de permettre `AWSServiceRoleForAWSShield` à Shield d'effectuer des actions en votre nom.

Shield Advanced permet d'utiliser cette politique lorsque vous activez l'atténuation automatique des attaques DDoS au niveau de l'application. Pour plus d'informations sur l'utilisation de cette politique, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

Pour plus d'informations sur le rôle lié à un service AWSServiceRoleForAWSShield qui utilise cette politique, voir Utilisation de rôles liés à un service pour Shield Advanced

Pour plus de détails sur cette politique, consultez AWSShieldServiceRolePolicyla console IAM.

Shield : mises à jour des politiques AWS gérées

Consultez les informations relatives aux mises à jour apportées aux politiques AWS gérées pour Shield depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des documents du Shield à l'adresseHistorique du document.

Politique	Description du changement	Date
`AWSShieldServiceRolePolicy` Cette politique permet à Shield d'accéder aux AWS ressources et de les gérer afin de répondre automatiquement aux attaques DDoS au niveau de la couche application en votre nom. Détails de la console IAM : AWSShieldServiceRolePolicy Le rôle lié au service `AWSServiceRoleForAWSShield` utilise cette politique. Pour plus d'informations, consultez Utilisation de rôles liés à un service pour Shield Advanced.	Cette politique a été ajoutée pour fournir à Shield Advanced les autorisations requises pour la fonctionnalité d'atténuation automatique des attaques DDoS au niveau de la couche applicative. Pour plus d'informations sur cette fonctionnalité, consultez Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.	1er décembre 2021
Shield a commencé à suivre les modifications	Shield a commencé à suivre les modifications apportées AWS à ses politiques gérées.	3 mars 2021

Résolution des problèmes AWS Shield d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Shield et IAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans Shield

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `shield:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 shield:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `shield:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Shield.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Shield. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les stratégies de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder à mes ressources Shield

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Shield prend en charge ces fonctionnalités, consultezComment AWS Shield fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Utilisation de rôles liés à un service pour Shield Advanced

AWS Shield Advanced utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Shield Advanced. Les rôles liés au service sont prédéfinis par Shield Advanced et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration de Shield Advanced, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Shield Advanced définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Shield Advanced peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège vos ressources Shield Advanced, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour Shield Advanced

Shield Advanced utilise le rôle lié au service nommé. AWSServiceRoleForAWSShield Ce rôle permet à Shield Advanced d'accéder aux AWS ressources et de les gérer afin de répondre automatiquement aux attaques DDoS au niveau de la couche application en votre nom. Pour plus d'informations sur cette fonctionnalité, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

Le rôle AWSServiceRoleForAWSShield lié à un service fait confiance aux services suivants pour assumer le rôle :

- `shield.amazonaws.com`

La politique d'autorisation des rôles nommée AWSShieldServiceRolePolicy permet à Shield Advanced d'effectuer les actions suivantes sur toutes les AWS ressources :

- `wafv2:GetWebACL`

- `wafv2:UpdateWebACL`
- `wafv2:GetWebACLForResource`
- `wafv2:ListResourcesForWebACL`
- `cloudfront:ListDistributions`
- `cloudfront:GetDistribution`

Lorsque des actions sont autorisées sur toutes les AWS ressources, cela est indiqué dans la politique sous la forme`"Resource": "*"`. Cela signifie uniquement que le rôle lié au service peut effectuer chaque action indiquée sur toutes les AWS ressources prises en charge par l'action. Par exemple, l'action n'`wafv2:GetWebACL`est prise en charge que pour les ressources ACL `wafv2` Web.

Shield Advanced effectue des appels d'API au niveau des ressources uniquement pour les ressources protégées pour lesquelles vous avez activé la fonctionnalité de protection de la couche d'application et pour les ACL Web associées à ces ressources protégées.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Création d'un rôle lié à un service pour Shield Advanced

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez l'atténuation automatique des attaques DDoS au niveau de la couche application pour une ressource de l'API AWS Management Console, de l' AWS CLI API ou de l' AWS API, Shield Advanced crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous activez l'atténuation automatique des attaques DDoS au niveau de la couche application pour une ressource, Shield Advanced crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour Shield Advanced

Shield Advanced ne vous permet pas de modifier le rôle AWSServiceRoleForAWSShield lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence à ce rôle. Néanmoins, vous pouvez modifier la

description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Shield Advanced

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si Shield Advanced utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources Shield Advanced utilisées par AWSServiceRoleForAWSShield

Pour toutes vos ressources pour lesquelles les protections DDoS de la couche application sont configurées, désactivez l'atténuation automatique des attaques DDoS au niveau de la couche application. Pour les instructions relatives à la console, voirConfiguration des protections DDoS au niveau de la couche applicative.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au AWSServiceRoleForAWSShield service. Pour plus d'informations, veuillez consulter Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés aux services Shield Advanced

Shield Advanced prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez la section Points de terminaison et quotas Shield Advanced.

Journalisation et surveillance dans Shield

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de Shield et de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. AWS fournit plusieurs outils pour surveiller les ressources de votre Shield et répondre à des événements potentiels :

CloudWatch Alarmes Amazon

À l'aide d' CloudWatch alarmes, vous observez une seule métrique sur une période que vous spécifiez. Si la métrique dépasse un seuil donné, CloudWatch envoie une notification à une rubrique ou AWS Auto Scaling à une politique Amazon SNS. Pour plus d’informations, consultez Surveillance avec Amazon CloudWatch.

AWS CloudTrail Journaux

CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Shield. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Shield, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite et des informations supplémentaires. Pour plus d'informations, voir Journalisation des appels d'API AWS CloudTrail avec.

Validation de conformité pour Shield

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

  > **Note**
  >
  > Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.

- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Resilience dans Shield

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l’infrastructure dans AWS Shield

En tant que service géré, AWS Shield il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Shield via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

AWS Shield Advanced quotas

AWS Shield Advanced dispose de quotas par défaut sur le nombre d'entités par région. Vous pouvez demander une augmentation de ces quotas.

Ressource	Quota par défaut
Nombre maximum de ressources protégées pour chaque type de ressource AWS Shield Advanced offrant une protection, par compte.	1 000
Nombre maximum de groupes de protection par compte.	100
Nombre maximal de ressources protégées individuelles que vous pouvez inclure spécifiquement dans un groupe de protection. Dans l'API, cela s'applique à celui `Members` que vous spécifiez lorsque vous définissez le groupe `Pattern` de protection sur`ARBITRARY` . Dans la console, cela s'applique aux ressources que vous sélectionnez pour le groupe de protection Choisissez parmi les ressources protégées.	1 000

AWS Firewall Manager

AWS Firewall Manager simplifie vos tâches d'administration et de maintenance sur plusieurs comptes et ressources pour diverses protections AWS WAF AWS Shield Advanced, notamment les groupes de sécurité Amazon VPC et les ACL réseau, AWS Network Firewall ainsi que le pare-feu DNS Amazon Route 53 Resolver. Avec Firewall Manager, vous configurez vos protections une seule fois et le service les applique automatiquement à tous vos comptes et ressources, même lorsque vous ajoutez de nouveaux comptes et ressources.

Firewall Manager offre ces avantages :

- Permet de protéger les ressources entre comptes
- Permet de protéger toutes les ressources d'un type particulier, telles que toutes les CloudFront distributions Amazon
- Permet de protéger toutes les ressources avec des balises spécifiques
- Ajoute automatiquement la protection aux ressources qui sont ajoutées à votre compte
- Vous permet d'abonner tous les comptes membres d'une AWS Organizations organisation à AWS Shield Advanced et d'abonner automatiquement les nouveaux comptes concernés qui rejoignent l'organisation
- Permet d'appliquer des règles de groupe de sécurité à tous les comptes membres ou sous-ensembles spécifiques de comptes d'une organisation AWS Organizations et applique automatiquement les règles aux nouveaux comptes concernés qui rejoignent l'organisation
- Vous permet d'utiliser vos propres règles ou d'acheter des règles gérées auprès de AWS Marketplace

Firewall Manager est particulièrement utile lorsque vous souhaitez protéger l'ensemble de votre organisation plutôt qu'un petit nombre de comptes et de ressources spécifiques, ou si vous ajoutez fréquemment de nouvelles ressources que vous souhaitez protéger. Firewall Manager fournit également une surveillance centralisée des attaques DDoS au sein de votre entreprise.

Rubriques

- Commencer à utiliser les AWS Firewall Manager politiques
- Travailler avec les AWS Firewall Manager politiques
- Utilisation des ensembles de ressources dans Firewall Manager
- Afficher les informations de conformité d'une AWS Firewall Manager politique
- AWS Firewall Manager résultats
- Sécurité dans votre utilisation du AWS Firewall Manager service
- AWS Firewall Manager quotas

AWS Firewall Manager tarification

Les frais engagés par AWS Firewall Manager concernent les services sous-jacents, tels que AWS WAF et AWS Config. Pour plus d'informations, consultez AWS Firewall Manager Pricing (Tarification CTlong).

AWS Firewall Manager prérequis

Cette rubrique explique comment vous préparer à administrer AWS Firewall Manager. Vous utilisez un compte administrateur Firewall Manager pour gérer toutes les politiques de sécurité de Firewall Manager de votre entreprise dans AWS Organizations. Sauf indication contraire, effectuez les étapes préalables en utilisant le compte que vous utiliserez en tant qu'administrateur de Firewall Manager.

Avant d'utiliser Firewall Manager pour la première fois, effectuez les étapes suivantes dans l'ordre.

Rubriques

- Étape 1 : Rejoindre et configurer AWS Organizations
- Étape 2 : créer un compte administrateur AWS Firewall Manager par défaut
- Étape 3 : activer AWS Config
- Étape 4 : Pour les politiques relatives aux tiers, abonnez-vous au AWS Marketplace et configurez les paramètres des tiers
- Étape 5 : Pour les politiques de Network Firewall et de DNS Firewall, activez le partage des ressources
- Étape 6 : À utiliser AWS Firewall Manager dans les régions désactivées par défaut

Étape 1 : Rejoindre et configurer AWS Organizations

Pour utiliser Firewall Manager, votre compte doit être membre de l'organisation du AWS Organizations service dans lequel vous souhaitez utiliser vos politiques de Firewall Manager.

> **Note**
>
> Pour plus d'informations sur les Organizations, consultez le Guide de AWS Organizations l'utilisateur.

Pour établir l' AWS Organizations adhésion et la configuration requises

1. Choisissez un compte à utiliser en tant qu'administrateur de Firewall Manager pour l'organisation dans Organizations.
2. Si le compte que vous avez choisi n'est pas encore membre de l'organisation, demandez-le d'y adhérer. Suivez les instructions de la section Inviter un Compte AWS homme à rejoindre votre organisation.
3. AWS Organizations propose deux ensembles de fonctionnalités : les fonctionnalités de facturation consolidée et toutes les fonctionnalités. Pour utiliser Firewall Manager, votre entreprise doit être activée pour toutes les fonctionnalités. Si votre organisation est configurée uniquement pour la facturation consolidée, suivez les instructions de la section Activation de toutes les fonctionnalités de votre organisation.

Étape 2 : créer un compte administrateur AWS Firewall Manager par défaut

Cette procédure utilise le compte et l'organisation que vous avez choisis et configurés à l'étape précédente.

Seul le compte de gestion de l'organisation peut créer des comptes d'administrateur par défaut de Firewall Manager. Le premier compte administrateur que vous créez est le compte administrateur par défaut. Le compte administrateur par défaut peut gérer des pare-feux tiers et dispose d'une portée administrative complète. Lorsque vous définissez le compte administrateur par défaut, Firewall Manager le définit automatiquement en tant qu'administrateur AWS Organizations délégué pour Firewall Manager. Cela permet à Firewall Manager d'accéder aux informations relatives aux unités organisationnelles (UO) de l'organisation. Vous pouvez utiliser des unités d'organisation pour définir l'étendue de vos politiques de Firewall Manager. Pour plus d'informations sur la définition

du champ d'application des politiques, consultez les instructions relatives aux différents types de politiques ci-dessousCréation d'une AWS Firewall Manager politique. Pour plus d'informations sur les organisations et les comptes de gestion, consultez Gérer les AWS comptes de votre organisation.

Paramètres requis pour le compte de gestion de l'organisation

Le compte de gestion de l'organisation doit disposer des paramètres suivants pour intégrer l'organisation à Firewall Manager et créer un administrateur par défaut :

- Il doit être membre de l'organisation dans AWS Organizations laquelle vous souhaitez appliquer vos politiques de Firewall Manager.

Pour définir le compte administrateur par défaut

1. Connectez-vous au Firewall Manager à l' AWS Management Console aide d'un compte AWS Organizations de gestion existant.
2. Ouvrez la console Firewall Manager à l'adresse https://console.aws.amazon.com/wafv2/fmsv2.
3. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
4. Entrez l'identifiant du AWS compte que vous avez choisi d'utiliser en tant qu'administrateur de Firewall Manager.

   > **Note**
   >
   > L'administrateur par défaut dispose d'un champ d'administration complet. L'étendue administrative complète signifie que ce compte peut appliquer des politiques à tous les comptes et unités organisationnelles (UO) de l'organisation, prendre des mesures dans toutes les régions et gérer tous les types de politiques de Firewall Manager.

5. Choisissez Créer un compte administrateur pour créer le compte.

Pour plus d'informations sur la gestion du compte administrateur de Firewall Manager, consultezTravailler avec AWS Firewall Manager les administrateurs.

Étape 3 : activer AWS Config

Pour utiliser Firewall Manager, vous devez l'activer AWS Config.

> **Note**
>
> Vous devez payer des frais pour vos AWS Config paramètres, conformément à la AWS Config tarification. Pour plus d'informations, consultez Getting Started with AWS Config.

> **Note**
>
> Pour que Firewall Manager puisse contrôler le respect des politiques, AWS Config il doit enregistrer en permanence les modifications de configuration des ressources protégées. Dans votre AWS Config configuration, la fréquence d'enregistrement doit être réglée sur Continuous, qui est le réglage par défaut.

AWS Config Pour activer Firewall Manager

1. Activez AWS Config cette option pour chacun de vos comptes AWS Organizations membres, y compris le compte administrateur de Firewall Manager. Pour plus d'informations, consultez Getting Started with AWS Config.
2. Activez Région AWS cette option AWS Config pour chaque élément contenant les ressources que vous souhaitez protéger. Vous pouvez l'activer AWS Config manuellement ou utiliser le AWS CloudFormation modèle « Activer AWS Config » dans la section AWS CloudFormation StackSets Exemples de modèles.

   Si vous ne souhaitez pas activer toutes AWS Config les ressources, vous devez activer les options suivantes en fonction du type de politiques de Firewall Manager que vous utilisez :

   - Politique WAF — Activez Config pour les types de ressources CloudFront Distribution, Application Load Balancer (ElasticLoadBalancingchoisissez V2 dans la liste), API Gateway, WAF WebACL, WAF Regional WebACL et WAFv2 WebACL. AWS Config Pour activer la protection d'une CloudFront distribution, vous devez vous trouver dans la région USA Est (Virginie du Nord). Les autres régions n'ont pas CloudFront d'option.
   - Politique de Shield — Activez Config pour les types de ressources Shield Protection, ShieldRegional Protection, Application Load Balancer, EC2 EIP, WAF WebACL, WAF Regional WebACL et WAFv2 WebACL.
   - Politique de groupe de sécurité — Activez Config pour les types de ressources EC2 SecurityGroup, EC2 Instance et EC2. NetworkInterface

- Politique ACL réseau — Activez Config pour les types de ressources Amazon EC2 Subnet et Amazon EC2 network ACL.
- Politique de pare-feu réseau : activez Config pour les types de ressources EC2 VPC NetworkFirewall FirewallPolicy NetworkFirewallRuleGroup, EC2, InternetGateway EC2 et EC2 RouteTable Subnet.
- Politique de pare-feu DNS — Activez Config pour le type de ressource EC2 VPC.
- Politique de pare-feu tierce : activez Config pour les types de ressources Amazon EC2 VPC, Amazon EC2, Amazon EC2, Amazon EC2, InternetGateway Amazon EC2 Subnet et Amazon EC2 RouteTable VPCEndpoint.

> **Note**
>
> Si vous configurez votre AWS Config enregistreur pour utiliser un rôle IAM personnalisé, vous devez vous assurer que la politique IAM dispose des autorisations appropriées pour enregistrer les types de ressources requis par la politique Firewall Manager. Sans les autorisations appropriées, les ressources requises risquent de ne pas être enregistrées, ce qui empêche Firewall Manager de protéger correctement vos ressources. Firewall Manager n'a aucune visibilité sur ces erreurs de configuration des autorisations. Pour plus d'informations sur l'utilisation d'IAM avec AWS Config, voir IAM for. AWS Config

Étape 4 : Pour les politiques relatives aux tiers, abonnez-vous au AWS Marketplace et configurez les paramètres des tiers

Remplissez les conditions préalables suivantes pour commencer à utiliser les politiques de pare-feu tierces de Firewall Manager.

Conditions préalables à la politique Fortigate Cloud Native Firewall (CNF) en tant que service

Pour utiliser Fortigate CNF pour Firewall Manager

1. Abonnez-vous au Fortigate Cloud Native Firewall (CNF) en tant que service sur le Marketplace. AWS

2. Enregistrez d'abord un locataire sur le portail des produits Fortigate CNF. Ajoutez ensuite votre compte administrateur Firewall Manager sous votre locataire sur le portail des produits Fortigate CNF. Pour plus d'informations, consultez la documentation Fortigate CNF.

Pour plus d'informations sur l'utilisation des politiques Fortigate CNF, consultez. Politiques de pare-feu natif du cloud (CNF) de Fortigate en tant que service

Conditions préalables à la politique de pare-feu de nouvelle génération de Palo Alto Networks Cloud

Pour utiliser Palo Alto Networks Cloud NGFW pour Firewall Manager

1. Abonnez-vous au service Pay-As-You-Go de Palo Alto Networks Cloud Next Generation Firewall sur le Marketplace. AWS
2. Suivez les étapes de déploiement du Palo Alto Networks Cloud NGFW répertoriées dans le Deploy Palo Alto Networks Cloud NGFW en suivant la AWS Firewall Manager rubrique du guide de déploiement du pare-feu de nouvelle AWS génération Palo Alto Networks Cloud Next Generation Firewall pour le déploiement. AWS

Pour plus d'informations sur l'utilisation des politiques NGFW Cloud de Palo Alto Networks, consultez. Politiques NGFW de Palo Alto Networks Cloud

Étape 5 : Pour les politiques de Network Firewall et de DNS Firewall, activez le partage des ressources

Pour gérer les politiques de Firewall Manager Network Firewall et de DNS Firewall, vous devez activer le partage avec AWS Organizations in AWS Resource Access Manager. Cela permet à Firewall Manager de déployer des protections sur l'ensemble de vos comptes lorsque vous créez ces types de politiques.

Pour activer le partage avec AWS OrganizationsAWS Resource Access Manager

- Suivez les instructions de la section Activer le partage avec AWS Organizations dans le guide de AWS Resource Access Manager l'utilisateur.

Si vous rencontrez des problèmes avec le partage des ressources, consultez les instructions à l'adresse Partage des ressources pour les politiques de Network Firewall et de DNS Firewall.

Étape 6 : À utiliser AWS Firewall Manager dans les régions désactivées par défaut

Pour utiliser Firewall Manager dans une région désactivée par défaut, vous devez activer la région à la fois pour le compte de gestion de votre AWS organisation et pour le compte administrateur par défaut de Firewall Manager. Pour plus d'informations sur les régions désactivées par défaut et sur la manière de les activer, consultez la section Gestion Régions AWS dans le manuel de référence AWS général.

Pour activer une région désactivée

- Pour le compte de gestion Organizations et le compte administrateur par défaut de Firewall Manager, suivez les instructions de la section Enabling a Region du AWS General Reference.

Après avoir suivi ces étapes, vous pouvez configurer Firewall Manager pour commencer à protéger vos ressources. Pour plus d'informations, voir Commencer à utiliser les AWS Firewall ManagerAWS WAF politiques.

Travailler avec AWS Firewall Manager les administrateurs

AWS Firewall Manager Vous pouvez avoir un ou plusieurs administrateurs capables de gérer les ressources de pare-feu de votre organisation. Si vous souhaitez utiliser plusieurs administrateurs Firewall Manager dans votre organisation, vous pouvez appliquer des conditions d'étendue administrative à chaque administrateur afin de définir les ressources qu'il peut gérer. Cela vous donne la flexibilité d'avoir différents rôles d'administrateur au sein de votre organisation et vous aide à conserver le principe de l'accès le moins privilégié. Par exemple, vous pouvez demander à un administrateur de gérer un ensemble d'unités organisationnelles (UO) pour votre organisation, tout en déléguant à un autre administrateur le soin de gérer uniquement des types de politiques spécifiques de Firewall Manager. Pour plus d'informations sur les organisations et les comptes de gestion, consultez Gérer les AWS comptes de votre organisation.

Pour connaître le nombre maximal d'administrateurs que vous pouvez avoir par organisation, voir AWS Firewall Manager quotas

Commencer à utiliser les administrateurs de Firewall Manager

Avant de commencer à utiliser les administrateurs de Firewall Manager, vous devez remplir les conditions requises répertoriées dansAWS Firewall Manager prérequis. Dans les conditions

préalables, vous allez intégrer une AWS Organizations organisation à Firewall Manager et créer un compte administrateur par défaut pour Firewall Manager. Un compte administrateur par défaut permet de gérer des pare-feux tiers et possède une portée administrative complète.

Champ d'application administratif

Le périmètre administratif définit les ressources que l'administrateur de Firewall Manager peut gérer. Une fois qu'un compte de AWS Organizations gestion a intégré une organisation à Firewall Manager, il peut créer des administrateurs Firewall Manager supplémentaires dotés de différents domaines d'administration. Un compte AWS Organizations de gestion peut accorder à l'administrateur un champ d'administration complet ou restreint. L'étendue complète donne à l'administrateur un accès complet à tous les types de ressources précédents. Le champ d'application restreint fait référence à l'octroi d'une autorisation administrative uniquement à un sous-ensemble des ressources précédentes. Nous vous recommandons de n'accorder aux administrateurs que les autorisations dont ils ont besoin pour accomplir les tâches liées à leur rôle. Vous pouvez appliquer n'importe quelle combinaison de ces conditions d'étendue administrative à un administrateur :

- Comptes ou unités d'organisation de votre organisation auxquels l'administrateur peut appliquer des politiques.
- Régions dans lesquelles l'administrateur peut effectuer des actions.
- Types de politiques Firewall Manager que l'administrateur peut gérer.

Rôles d'administrateur

Il existe deux types de rôles d'administrateur dans Firewall Manager : un administrateur par défaut et des administrateurs de Firewall Manager.

- Administrateur par défaut : le compte de gestion de l'organisation crée un compte administrateur par défaut de Firewall Manager lorsqu'il intègre son organisation à Firewall Manager alors qu'il termine leAWS Firewall Manager prérequis. L'administrateur par défaut peut gérer des pare-feux tiers et dispose d'une portée administrative complète, mais il se trouve au même niveau que les autres administrateurs, si vous choisissez d'avoir plusieurs administrateurs.
- Administrateurs de Firewall Manager : un administrateur de Firewall Manager peut gérer les ressources que le compte de AWS Organizations gestion lui désigne dans la configuration de son étendue administrative. Pour connaître le nombre maximal d'administrateurs que vous pouvez avoir par organisation, consultezAWS Firewall Manager quotas. Lors de la création d'un compte administrateur de Firewall Manager, le service vérifie si le compte est déjà un administrateur délégué pour Firewall Manager au sein de l'organisation. AWS Organizations

Dans le cas contraire, Firewall Manager appelle Organizations pour définir le compte en tant qu'administrateur délégué pour Firewall Manager. Pour plus d'informations sur les administrateurs délégués des Organisations, consultez AWS Organizations la terminologie et les concepts du Guide de AWS Organizations l'utilisateur.

Administrateurs existants

Si vous êtes déjà client de Firewall Manager et que vous avez déjà défini un administrateur, cet administrateur existant sera l'administrateur par défaut de Firewall Manager. Il ne devrait y avoir aucun impact sur votre flux existant. Si vous souhaitez ajouter d'autres administrateurs, vous pouvez le faire en suivant les procédures décrites dans ce chapitre.

Création, mise à jour et révocation de comptes d'administrateur de Firewall Manager

Les procédures décrites dans les rubriques suivantes expliquent comment créer, mettre à jour et révoquer des comptes d'administrateur de Firewall Manager. Seul le compte de gestion d'une entreprise peut créer et mettre à jour des comptes d'administrateur de Firewall Manager. Seul un administrateur individuel de Firewall Manager peut révoquer son propre compte d'administrateur.

Création d'un compte administrateur de Firewall Manager

La procédure suivante décrit comment créer un compte administrateur de Firewall Manager à l'aide de la console Firewall Manager.

Pour créer un compte administrateur de Firewall Manager

1. Connectez-vous au Firewall Manager à l' AWS Management Console aide d'un compte AWS Organizations de gestion existant.
2. Ouvrez la console Firewall Manager à l'adresse https://console.aws.amazon.com/wafv2/fmsv2.
3. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
4. Choisissez Créer un compte administrateur.
5. Dans le volet Détails, dans le AWS champ ID du compte, saisissez l' AWS ID du compte membre que vous souhaitez ajouter en tant qu'administrateur de Firewall Manager.
6. Pour le champ d'application administratif, choisissez l'une des options suivantes :

   - Complet — Cela permet à l'administrateur d'appliquer des politiques à tous les comptes et unités organisationnelles (UO) de l'organisation, de prendre des mesures dans toutes les

régions et d'appliquer tous les types de politiques de Firewall Manager, à l'exception des pare-feux tiers. Seul l'administrateur par défaut peut créer et gérer des pare-feux tiers. Soyez prudent si vous accordez ce niveau d'autorisations à l'administrateur. Dans l'esprit du moindre privilège, nous recommandons de n'accorder à l'administrateur que les autorisations dont il a besoin pour accomplir les tâches liées à son rôle.

- Restreint : si vous appliquez une étendue restreinte, dans Configurer l'étendue administrative, configurez les comptes et les unités organisationnelles, les régions et les types de politiques que le compte peut gérer.

  Pour les comptes et les unités organisationnelles, choisissez les options suivantes :

  - Si vous souhaitez appliquer des politiques à tous les comptes ou unités organisationnelles de votre organisation, choisissez Inclure tous les comptes dans mon AWS organisation.
  - Si vous souhaitez appliquer des politiques uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.
  - Si vous souhaitez appliquer des politiques à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

  Pour les régions, choisissez les options suivantes :

  - Si vous souhaitez autoriser l'administrateur à effectuer des actions dans toutes les régions disponibles, choisissez Inclure toutes les régions.
  - Si vous souhaitez que l'administrateur n'effectue des actions que dans des régions spécifiques, choisissez Inclure uniquement les régions spécifiées, puis spécifiez les régions que vous souhaitez inclure.

> **Note**
>
> Pour inclure une région désactivée par défaut, vous devez activer la région à la fois pour le compte de gestion de l' AWS Organizations organisation et pour le compte d'administration par défaut. Pour plus d'informations sur l'activation des régions pour un compte, voir Activer une région dans le Référence générale d'Amazon Web Services.

Pour les types de politiques, choisissez les options suivantes :

- Si vous souhaitez autoriser l'administrateur à gérer tous les types de politiques, choisissez Inclure tous les types de politiques.
- Si vous souhaitez que l'administrateur ne gère que des types de politiques spécifiques, choisissez Inclure uniquement les types de stratégie spécifiés, puis spécifiez les types de stratégie que vous souhaitez inclure.

7. Choisissez Créer un compte administrateur pour créer le compte administrateur. Lors de la création, Firewall Manager appelle AWS Organizations pour savoir si l'administrateur est déjà un administrateur délégué de votre organisation. Dans le cas contraire, Firewall Manager désignera le compte en tant qu'administrateur délégué. Pour plus d'informations sur les administrateurs délégués dans Organizations, reportez-vous à AWS Organizations la terminologie et aux concepts du Guide de AWS Organizations l'utilisateur.

Si vous appliquez une portée administrative restreinte, Firewall Manager évalue automatiquement les nouvelles ressources par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager inclut automatiquement le compte dans le périmètre administratif.

Mettre à jour un compte administrateur de Firewall Manager

La procédure suivante décrit comment mettre à jour un compte administrateur de Firewall Manager à l'aide de la console Firewall Manager.

> **Note**
>
> Pour mettre à jour le champ d'application d'un administrateur afin d'inclure une région désactivée par défaut, vous devez activer la région à la fois pour le compte de gestion de AWS Organizations l'organisation et pour le compte d'administration par défaut. Pour plus d'informations sur l'activation des régions pour un compte, voir Activer une région dans le Référence générale d'Amazon Web Services.

Pour mettre à jour un compte administrateur (console)

1. Connectez-vous au Firewall Manager à l' AWS Management Console aide d'un compte AWS Organizations de gestion existant.
2. Ouvrez la console Firewall Manager à l'adresse https://console.aws.amazon.com/wafv2/fmsv2.
3. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
4. dans le tableau des administrateurs de Firewall Manager, choisissez le compte que vous souhaitez mettre à jour.
5. Sélectionnez Modifier pour modifier les informations du compte de l'administrateur. Vous ne pouvez pas modifier l'identifiant du compte.
6. Choisissez Save pour enregistrer les changements.

Révocation d'un compte administrateur

La procédure suivante décrit comment révoquer un compte administrateur de Firewall Manager. Si vous êtes l'administrateur par défaut, avant de pouvoir révoquer votre compte, tous les comptes administrateurs de Firewall Manager au sein de votre organisation doivent d'abord révoquer leurs propres comptes. Pour révoquer un compte administrateur, suivez la procédure ci-dessous

Pour révoquer un compte administrateur (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.
2. Dans le panneau de navigation, sélectionnez Settings (Paramètres).

3. Dans le volet Compte administrateur, sélectionnez Révoquer le compte administrateur pour révoquer votre compte.

> **Important**
>
> Lorsque vous révoquez les privilèges d'administrateur d'un compte administrateur, toutes les politiques de Firewall Manager créées par ce compte sont supprimées.

Modification du compte administrateur par défaut

Vous ne pouvez désigner qu'un seul compte dans une organisation comme compte administrateur par défaut de Firewall Manager. Le compte administrateur par défaut suit le principe du premier entré, dernier sorti. Pour désigner un compte administrateur par défaut différent, chaque compte administrateur doit d'abord révoquer son propre compte. L'administrateur par défaut existant peut alors révoquer son propre compte, ce qui aura également pour effet de déconnecter l'organisation de Firewall Manager. Lorsqu'un administrateur révoque son compte, toutes les politiques de Firewall Manager créées par ce compte sont supprimées. Pour désigner un nouveau compte administrateur par défaut, vous devez ensuite vous connecter à Firewall Manager avec le compte AWS Organizations de gestion afin de désigner un nouveau compte administrateur. Pour modifier le compte administrateur par défaut d'une organisation, effectuez la procédure suivante.

Pour modifier le compte administrateur par défaut

1. Connectez-vous au Firewall Manager à l' AWS Management Console aide d'un compte AWS Organizations de gestion existant.
2. Ouvrez la console Firewall Manager à l'adresse https://console.aws.amazon.com/wafv2/fmsv2.
3. Dans le panneau de navigation, sélectionnez Settings (Paramètres).
4. Entrez l'ID du compte que vous avez choisi d'utiliser en tant qu'administrateur de Firewall Manager.

> **Note**
>
> Ce compte est autorisé à créer et à gérer les politiques de Firewall Manager pour tous les comptes de votre organisation.

5. Choisissez Créer un compte administrateur.

6. Entrez l' AWS ID du compte que vous avez choisi d'utiliser en tant qu'administrateur de Firewall Manager.

> **Note**
>
> Ce compte dispose d'un champ d'application administratif complet. L'étendue administrative complète signifie que ce compte peut appliquer des politiques à tous les comptes et unités organisationnelles (UO) de l'organisation, prendre des mesures dans toutes les régions et gérer tous les types de politiques de Firewall Manager.

7. Choisissez Créer un compte administrateur pour créer le compte administrateur par défaut.

Disqualification des modifications apportées à un compte administrateur

Certaines modifications apportées à un compte administrateur peuvent empêcher celui-ci de rester un compte administrateur.

Cette section décrit les modifications susceptibles de disqualifier un compte administrateur, ainsi que la manière dont AWS Firewall Manager gère ces modifications.

Compte supprimé de l'organisation dans AWS Organizations

Si le compte AWS Firewall Manager administrateur est supprimé de l'organisation dans AWS Organizations, il ne peut plus administrer les politiques de l'organisation. Firewall Manager effectue l'une des actions suivantes :

- Compte sans politiques — Si le compte administrateur de Firewall Manager n'a aucune politique de Firewall Manager, Firewall Manager révoque le compte administrateur.
- Compte avec politiques de Firewall Manager — Si le compte administrateur de Firewall Manager possède des politiques de Firewall Manager, Firewall Manager vous envoie un e-mail pour vous informer de la situation et vous proposer les options que vous pouvez prendre, avec l'aide de votre responsable AWS commercial.

Compte fermé

Si vous fermez le compte que vous utilisez pour l' AWS Firewall Manager administrateur AWS et que Firewall Manager gère la fermeture comme suit :

- AWS révoque l'accès administrateur du compte depuis Firewall Manager et Firewall Manager désactive toutes les politiques gérées par le compte administrateur. Les protections fournies par ces politiques sont supprimées dans l'ensemble de l'organisation.
- AWS conserve les données de politique de Firewall Manager relatives au compte pendant 90 jours à compter de la date effective de fermeture du compte administrateur. Pendant cette période de 90 jours, vous pouvez rouvrir le compte fermé.
  - Si vous rouvrez le compte fermé pendant la période de 90 jours, AWS réassignez le compte en tant qu'administrateur de Firewall Manager et récupérez les données de politique de Firewall Manager relatives au compte.
  - Sinon, à la fin de la période de 90 jours, toutes les données de politique de Firewall Manager relatives au compte sont AWS définitivement supprimées.

Commencer à utiliser les AWS Firewall Manager politiques

Vous pouvez l' AWS Firewall Manager utiliser pour activer différents types de politiques de sécurité. Les étapes de configuration sont légèrement différentes pour chacun de ces éléments.

Rubriques

Commencer à utiliser les AWS Firewall ManagerAWS WAF politiques

AWS Firewall Manager Pour activer les AWS WAF règles au sein de votre organisation, effectuez les étapes suivantes dans l'ordre.

Rubriques

Étape 1 : Exécuter les prérequis

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez toutes les conditions préalables avant de passer à Étape 2 : créer et appliquer une AWS WAF politique.

Étape 2 : créer et appliquer une AWS WAF politique

Une AWS WAF politique Firewall Manager contient les groupes de règles que vous souhaitez appliquer à vos ressources. Firewall Manager crée une ACL Web Firewall Manager dans chaque compte sur lequel vous appliquez la politique. Les gestionnaires de comptes individuels peuvent ajouter des règles et des groupes de règles à la liste ACL web résultante, en plus des groupes de règles que vous définissez ici. Pour plus d'informations sur les AWS WAF politiques de Firewall Manager, consultezAWS WAF politiques.

Pour créer une AWS WAF politique Firewall Manager (console)

Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

1. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
2. Choisissez Créer une politique.
3. Pour Policy type (Type de stratégie), choisissez AWS WAF.
4. Pour Région, choisissez un Région AWS. Pour protéger les CloudFront distributions Amazon, choisissez Global.

   Pour protéger les ressources dans plusieurs régions (autres que les CloudFront distributions), vous devez créer des politiques Firewall Manager distinctes pour chaque région.
5. Choisissez Suivant.
6. Dans Nom de la politique, entrez un nom descriptif. Firewall Manager inclut le nom de la politique dans les noms des ACL Web qu'il gère. Les noms des ACL Web sont

`FMManagedWebACLV2-` suivis du nom de la politique que vous entrez ici et de l'horodatage de création des ACL Web, en millisecondes UTC. - Par exemple, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

> **Important**
>
> Les noms des ACL Web ne peuvent pas changer après leur création. Si vous mettez à jour le nom de votre politique, Firewall Manager ne mettra pas à jour le nom de l'ACL Web associé. Pour que Firewall Manager crée une ACL Web portant un nom différent, vous devez créer une nouvelle politique.

7. Sous Policy rules (Règles de stratégie), pour First rule groups (Premiers groupes de règles), choisissez Add rule groups (Ajouter des groupes de règles). Développez les groupes de règles AWS gérés. Pour Core rule set (Ensemble de règles de base), activez l'option Add to web ACL (Ajouter à la liste ACL web). Pour les entrées erronées AWS connues, activez l'option Ajouter à l'ACL Web. Choisissez Add rules (Ajouter des règles).

   Pour Last rule groups (Derniers groupes de règles), choisissez Add rule groups (Ajouter des groupes de règles). Développez les groupes de règles AWS gérés et, pour la liste de réputation d'Amazon IP, activez l'option Ajouter à l'ACL Web. Choisissez Add rules (Ajouter des règles).

   Sous Premiers groupes de règles, sélectionnez Ensemble de règles de base et choisissez Déplacer vers le bas. AWS WAF évalue les requêtes Web par rapport au groupe de règles relatives aux entrées erronées AWS connues avant de les évaluer par rapport à l'ensemble de règles de base.

   Vous pouvez également créer vos propres groupes de AWS WAF règles si vous le souhaitez à l'aide de la AWS WAF console. Tous les groupes de règles que vous créez apparaissent sous Vos groupes de règles dans la page Describe policy : Add rule groups (Décrire la stratégie : Ajouter des groupes de règles).

   Les premier et dernier groupes de AWS WAF règles que vous gérez via Firewall Manager ont des noms qui commencent respectivement par `PREFMManaged-` ou `POSTFMManaged-` sont suivis du nom de la politique de Firewall Manager et de l'horodatage de création du groupe de règles, en millisecondes UTC. Par exemple, `PREFMManaged-MyWAFPolicyName-1621880555123`.
8. Conservez l'action par défaut Autoriser pour la liste ACL web.

9. Conservez la valeur par défaut de Policy action (Action de stratégie), pour ne pas corriger automatiquement les ressources non conformes. Vous pouvez modifier cette option ultérieurement.
10. Choisissez Suivant.
11. Pour Policy scope (Étendue de la stratégie), vous fournissez les paramètres pour les comptes, les types de ressources et le balisage qui identifient les ressources auxquelles vous souhaitez appliquer la stratégie. Pour ce didacticiel, quittez les paramètres Comptes AWSet Ressources, puis choisissez un ou plusieurs types de ressources.
12. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.
13. Choisissez Suivant.
14. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
15. Choisissez Suivant.
16. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Vérifiez que Policy action (Action de stratégie) est défini sur Identify resources that don’t comply with the policy rules, but don’t auto remediate (Identifier les ressources qui ne sont pas conformes aux règles de stratégie, mais ne pas effectuer une résolution automatique). Cela vous permet de passer en revue les modifications que votre politique apporterait avant de les activer.
17. Lorsque vous êtes satisfait de la politique, choisissez Créer une politique.

    Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du

paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

Étape 3 : Nettoyage

Pour éviter des frais superflus, supprimez les stratégies et ressources inutiles.

Pour supprimer une stratégie (console)

1. Sur la page AWS Firewall Manager des politiques, cliquez sur le bouton radio à côté du nom de la politique, puis sélectionnez Supprimer.
2. Dans la zone de confirmation Supprimer, sélectionnez Delete all policy resources (Supprimer toutes les ressources de stratégie), puis choisissez à nouveau Supprimer.

   AWS WAF supprime la politique et toutes les ressources associées, telles que les ACL Web, qu'elle a créées dans votre compte. La propagation des modifications à tous les comptes peut prendre quelques minutes.

Commencer à utiliser les AWS Firewall ManagerAWS Shield Advanced politiques

Vous pouvez l'utiliser AWS Firewall Manager pour activer AWS Shield Advanced les protections au sein de votre organisation.

> **Important**
>
> Firewall Manager ne prend pas en charge Amazon Route 53 ou AWS Global Accelerator. Si vous devez protéger ces ressources avec Shield Advanced, vous ne pouvez pas utiliser une politique Firewall Manager. Au lieu de cela, suivez les instructions de Ajouter AWS Shield Advanced une protection aux AWS ressources.

Pour utiliser Firewall Manager afin d'activer la protection Shield Advanced, effectuez les étapes suivantes dans l'ordre.

Rubriques

Étape 1 : Exécuter les prérequis

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez toutes les conditions préalables avant de passer à Étape 2 : créer et appliquer une politique Shield Advanced.

Étape 2 : créer et appliquer une politique Shield Advanced

Après avoir rempli les conditions requises, vous créez une politique AWS Firewall Manager Shield Advanced. Une politique Firewall Manager Shield Advanced contient les comptes et les ressources que vous souhaitez protéger avec Shield Advanced.

> **Important**
>
> Firewall Manager ne prend pas en charge Amazon Route 53 ou AWS Global Accelerator. Si vous devez protéger ces ressources avec Shield Advanced, vous ne pouvez pas utiliser une politique Firewall Manager. Au lieu de cela, suivez les instructions de Ajouter AWS Shield Advanced une protection aux AWS ressources.

Pour créer une politique Firewall Manager Shield Advanced (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour le type de politique, choisissez Shield Advanced.

   Pour créer une politique Shield Advanced, votre compte administrateur Firewall Manager doit être abonné à Shield Advanced. Si vous n'êtes pas abonné, vous êtes invité à le faire. Pour plus d'informations sur le coût de l'abonnement, consultez la section AWS Shield Advanced Tarification.

   > **Note**
   >
   > Il n'est pas nécessaire d'inscrire manuellement chaque compte membre à Shield Advanced. Firewall Manager le fait pour vous lorsqu'il crée la politique. Chaque compte doit rester abonné à Firewall Manager et à Shield Advanced pour continuer à protéger les ressources du compte.

5. Pour Région, choisissez un Région AWS. Pour protéger les CloudFront ressources d'Amazon, choisissez Global.

   Pour protéger les ressources de plusieurs régions (autres que les CloudFront ressources), vous devez créer des politiques Firewall Manager distinctes pour chaque région.
6. Choisissez Suivant.
7. Dans Nom, entrez un nom descriptif.
8. (Région mondiale uniquement) Pour les politiques régionales mondiales, vous pouvez choisir si vous souhaitez gérer l'atténuation automatique des attaques DDoS au niveau de la couche d'application Shield Advanced. Pour ce didacticiel, conservez le paramètre par défaut Ignorer pour ce choix.
9. Pour l'action stratégique, choisissez l'option qui ne corrige pas automatiquement.
10. Choisissez Suivant.
11. Comptes AWS cette politique s'applique pour vous permettre de réduire le champ d'application de votre politique en spécifiant les comptes à inclure ou à exclure. Pour ce didacticiel, choisissez Include all accounts under my organization (Inclure tous les comptes de mon organisation).
12. Choisissez les types de ressource que vous voulez protéger.

    Firewall Manager ne prend pas en charge Amazon Route 53 ou AWS Global Accelerator. Si vous devez protéger ces ressources avec Shield Advanced, vous ne pouvez pas utiliser une

politique Firewall Manager. Suivez plutôt les instructions de Shield Advanced à l'adresseAjouter AWS Shield Advanced une protection aux AWS ressources.

13. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.

14. Choisissez Suivant.
15. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
16. Choisissez Suivant.
17. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Vérifiez que Policy action (Action de stratégie) est défini sur Identify resources that don't comply with the policy rules, but don't auto remediate (Identifier les ressources qui ne sont pas conformes aux règles de stratégie, mais ne pas effectuer une résolution automatique). Cela vous permet de passer en revue les modifications que votre politique apporterait avant de les activer.

18. Lorsque vous êtes satisfait de la politique, choisissez Créer une politique.

    Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

Passez au Étape 3 : (Facultatif) autorisez la Shield Response Team (SRT).

Étape 3 : (Facultatif) autorisez la Shield Response Team (SRT)

L'un des avantages AWS Shield Advanced est le soutien de la Shield Response Team (SRT). Lorsque vous êtes victime d'une attaque DDoS potentielle, vous pouvez contacter le AWS Support Centre. Si nécessaire, le Support Center transmet votre problème au SRT. Le SRT vous aide à analyser les activités suspectes et à atténuer le problème. Cette atténuation implique souvent de créer ou de mettre à jour AWS WAF des règles et des ACL Web dans votre compte. Le SRT peut inspecter votre AWS WAF configuration et créer ou mettre à jour des AWS WAF règles et des ACL Web pour vous, mais l'équipe a besoin de votre autorisation pour le faire. Dans le cadre de la configuration AWS Shield Advanced, nous vous recommandons de fournir à la SRT les autorisations nécessaires de manière proactive. La fourniture préalable de l'autorisation permet d'éviter les retards d'atténuation des risques en cas d'attaque réelle.

Vous autorisez et contactez le SRT au niveau du compte. C'est-à-dire que le propriétaire du compte, et non l'administrateur de Firewall Manager, doit effectuer les étapes suivantes pour autoriser le SRT à atténuer les attaques potentielles. L'administrateur de Firewall Manager ne peut autoriser le SRT que pour les comptes qu'il possède. De même, seul le titulaire du compte peut contacter le SRT pour obtenir de l'aide.

> **Note**
>
> Pour utiliser les services du SRT, vous devez être abonné au plan Business Support ou au plan Enterprise Support.

Pour autoriser le SRT à atténuer les attaques potentielles en votre nom, suivez les instructions figurant dansAssistance de la Shield Response Team (SRT). Vous pouvez modifier l'accès et les autorisations SRT à tout moment en suivant les mêmes étapes.

Passez au Étape 4 : configurer les notifications Amazon SNS et les alarmes Amazon CloudWatch .

Étape 4 : configurer les notifications Amazon SNS et les alarmes Amazon CloudWatch

Vous pouvez continuer à partir de cette étape sans configurer les notifications ou CloudWatch les alarmes Amazon SNS. Cependant, la configuration de ces alarmes et notifications augmente considérablement votre visibilité sur les éventuels événements DDoS.

Vous pouvez surveiller vos ressources protégées pour détecter d'éventuelles activités DDoS à l'aide d'Amazon SNS. Pour recevoir une notification concernant d'éventuelles attaques, créez une rubrique Amazon SNS pour chaque région.

Pour créer une rubrique Amazon SNS dans Firewall Manager (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sous AWS FMS, sélectionnez Paramètres.
3. Choisissez Create new topic (Créer une rubrique).
4. Saisissez un nom de rubrique.
5. Entrez l'adresse e-mail à laquelle les messages Amazon SNS seront envoyés, puis choisissez Ajouter une adresse e-mail.
6. Choisissez Update SNS configuration (Mettre à jour la configuration SNS).

Configurer les CloudWatch alarmes Amazon

Shield Advanced enregistre les indicateurs de détection, d'atténuation et des principaux contributeurs CloudWatch que vous pouvez surveiller. Pour plus d'informations, consultezAWS Shield Advanced métriques. CloudWatch entraîne des coûts supplémentaires. Pour CloudWatch connaître les tarifs, consultez Amazon CloudWatch Pricing.

Pour créer une CloudWatch alarme, suivez les instructions de la section Utilisation d'Amazon CloudWatch Alarms. Par défaut, Shield Advanced est configuré CloudWatch pour vous avertir après un seul indicateur d'un éventuel événement DDoS. Si nécessaire, vous pouvez utiliser la CloudWatch console pour modifier ce paramètre afin de ne vous avertir qu'après la détection de plusieurs indicateurs.

> **Note**
>
> Outre les alarmes, vous pouvez également utiliser un CloudWatch tableau de bord pour surveiller les activités DDoS potentielles. Le tableau de bord collecte et traite les données brutes de Shield Advanced en indicateurs lisibles en temps quasi réel. Vous pouvez utiliser les statistiques CloudWatch d'Amazon pour avoir une idée des performances de votre application ou service Web. Pour plus d'informations, consultez le contenu CloudWatch du guide de CloudWatch l'utilisateur Amazon.
> Pour obtenir des instructions sur la création d'un CloudWatch tableau de bord, consultezSurveillance avec Amazon CloudWatch. Pour plus d'informations sur les métriques spécifiques de Shield Advanced que vous pouvez ajouter à votre tableau de bord, consultezAWS Shield Advanced métriques.

Lorsque vous aurez terminé votre configuration Shield Advanced, familiarisez-vous avec les options de visualisation des événements surVisibilité sur les événements DDoS.

Commencer à utiliser les AWS Firewall Manager politiques des groupes de sécurité Amazon VPC

AWS Firewall Manager Pour activer les groupes de sécurité Amazon VPC au sein de votre organisation, effectuez les étapes suivantes dans l'ordre.

Rubriques

- Étape 1 : Exécuter les prérequis
- Étape 2 : Créer un groupe de sécurité à utiliser dans votre stratégie
- Étape 3 : créer et appliquer une politique de groupe de sécurité commune

Étape 1 : Exécuter les prérequis

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez toutes les conditions préalables avant de passer à Étape 2 : Créer un groupe de sécurité à utiliser dans votre stratégie.

Étape 2 : Créer un groupe de sécurité à utiliser dans votre stratégie

Au cours de cette étape, vous créez un groupe de sécurité que vous pouvez appliquer à l'ensemble de votre organisation à l'aide de Firewall Manager.

> **Note**
>
> Pour ce didacticiel, vous n'appliquerez pas votre stratégie de groupe de sécurité aux ressources de votre organisation. Vous allez simplement créer la stratégie et voir ce qui se passerait si vous appliquiez le groupe de sécurité de la stratégie à vos ressources. Pour ce faire, désactivez la résolution automatique sur la stratégie.

Si vous avez déjà un groupe de sécurité général défini, ignorez cette étape et passez à Étape 3 : créer et appliquer une politique de groupe de sécurité commune.

Pour créer un groupe de sécurité à utiliser dans une stratégie de groupe de sécurité commune de Firewall Manager

- Créez un groupe de sécurité que vous pouvez appliquer à tous les comptes et ressources de votre organisation, en suivant les instructions de la section Groupes de sécurité pour votre VPC dans le guide de l'utilisateur Amazon VPC.

  Pour plus d'informations sur les options de règles de groupe de sécurité, consultez Référence des règles de groupe de sécurité.

Vous êtes maintenant prêt à passer à Étape 3 : créer et appliquer une politique de groupe de sécurité commune.

Étape 3 : créer et appliquer une politique de groupe de sécurité commune

Après avoir rempli les conditions requises, vous créez une stratégie de groupe de sécurité AWS Firewall Manager commune. Une politique de groupe de sécurité commune fournit un groupe de sécurité contrôlé de manière centralisée pour AWS l'ensemble de votre organisation. Il définit également les ressources Comptes AWS et auxquelles le groupe de sécurité s'applique. Outre les politiques de groupe de sécurité communes, Firewall Manager prend en charge les politiques des groupes de sécurité d'audit de contenu, pour gérer les règles de groupe de sécurité utilisées dans votre organisation, et utilise les politiques des groupes de sécurité d'audit pour gérer les groupes

de sécurité inutilisés et redondants. Pour plus d'informations, consultez Politiques des groupes de sécurité.

Pour ce didacticiel, vous créez une stratégie de groupe de sécurité commune et vous définissez son action de manière à ne pas effectuer une résolution automatique. Cela vous permet de voir quel effet la politique aurait sans apporter de modifications à votre AWS organisation.

Pour créer une politique de groupe de sécurité commune de Firewall Manager (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Si vous n'avez pas respecté les prérequis, la console affiche les instructions sur la façon de corriger les problèmes. Suivez les instructions, puis revenez à cette étape, pour créer une stratégie de groupe de sécurité commune.
4. Choisissez Créer une politique.
5. Pour Type de stratégie, choisissez Groupe de sécurité.
6. Pour Security group policy type (Type de stratégie de groupe de sécurité), choisissez Common security groups (Groupes de sécurité communs).
7. Pour Région, choisissez un Région AWS.
8. Choisissez Suivant.
9. Dans Nom de la politique, entrez un nom descriptif.
10. Les Règles de stratégie vous permettent de choisir la manière dont les groupes de sécurité de cette stratégie sont appliqués et gérés. Pour ce didacticiel, laissez les options décochées.
11. Choisissez Add primary security group (Ajouter un groupe de sécurité principal), sélectionnez le groupe de sécurité que vous avez créé pour ce didacticiel, puis choisissez Add security group (Ajouter le groupe de sécurité).

12. Pour Policy action (Action de stratégie), choisissez Identify resources that don’t comply with the policy rules, but don’t auto remediate (Identifier les ressources qui ne sont pas conformes aux règles de stratégie, mais ne pas effectuer une résolution automatique).
13. Choisissez Suivant.
14. Comptes AWS concerné par cette politique vous permet de réduire le champ d'application de votre politique en spécifiant les comptes à inclure ou à exclure. Pour ce didacticiel, choisissez Include all accounts under my organization (Inclure tous les comptes de mon organisation).
15. Pour Type de ressource, choisissez un ou plusieurs types, en fonction des ressources que vous avez définies pour votre AWS organisation.
16. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.
17. Choisissez Suivant.
18. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
19. Choisissez Suivant.
20. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Vérifiez que Policy action (Action de stratégie) est défini sur Identify resources that don’t comply with the policy rules, but don’t auto remediate (Identifier les ressources qui ne sont pas conformes aux règles de stratégie, mais ne pas effectuer une résolution automatique). Cela vous permet de passer en revue les modifications que votre politique apporterait avant de les activer.
21. Lorsque vous êtes satisfait de la politique, choisissez Créer une politique.

Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

22. Lorsque vous avez terminé cette exploration, si vous ne souhaitez pas conserver la stratégie que vous avez créée pour ce didacticiel, choisissez le nom de la stratégie, Delete (Supprimer), Clean up resources created by this policy (Nettoyer les ressources créées par cette stratégie), puis enfin Delete (Supprimer).

Pour plus d'informations sur les politiques des groupes de sécurité de Firewall Manager, consultezPolitiques des groupes de sécurité.

Commencer à utiliser les AWS Firewall Manager politiques ACL du réseau Amazon VPC

AWS Firewall Manager Pour activer les ACL réseau au sein de votre organisation, effectuez les étapes décrites dans cette section dans l'ordre.

Pour plus d'informations sur les ACL réseau, consultez la section Contrôler le trafic vers les sous-réseaux à l'aide des ACL réseau dans le guide de l'utilisateur Amazon VPC.

Rubriques

- Étape 1 : Exécuter les prérequis
- Étape 2 : Création d'une politique ACL réseau

Étape 1 : Exécuter les prérequis

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez toutes les conditions préalables avant de passer à Étape 2 : Création d'une politique ACL réseau.

Étape 2 : Création d'une politique ACL réseau

Après avoir rempli les conditions requises, vous créez une politique ACL réseau Firewall Manager. Une politique d'ACL réseau fournit une définition d'ACL réseau contrôlée de manière centralisée pour AWS l'ensemble de votre organisation. Il définit également les sous-réseaux Comptes AWS et auxquels s'applique l'ACL du réseau.

Pour plus d'informations sur les politiques ACL du réseau Firewall Manager, consultezPolitiques ACL du réseau.

Pour des informations générales sur les politiques ACL du réseau Firewall Manager, consultezPolitiques ACL du réseau.

> **Note**
>
> Dans le cadre de ce didacticiel, vous n'appliquerez pas votre politique ACL réseau aux sous-réseaux de votre organisation. Vous allez simplement créer la politique et voir ce qui se passerait si vous appliquiez l'ACL réseau de la politique à vos sous-réseaux. Pour ce faire, désactivez la résolution automatique sur la stratégie.

Pour créer une politique ACL réseau Firewall Manager (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Si vous n'avez pas respecté les prérequis, la console affiche les instructions sur la façon de corriger les problèmes. Suivez les instructions, puis revenez à cette étape pour créer une politique ACL réseau.
4. Choisissez Créer une politique.

5. Pour Région, choisissez un Région AWS.
6. Pour le type de stratégie, choisissez Network ACL.
7. Choisissez Suivant.
8. Dans Nom de la politique, entrez un nom descriptif.
9. Pour les règles de politique ACL du réseau, définissez les première et dernière règles pour le trafic entrant et sortant.

   Vous définissez les règles ACL du réseau dans Firewall Manager de la même manière que vous les définissez via Amazon VPC. La seule différence est qu'au lieu d'attribuer vous-même des numéros de règles, vous attribuez l'ordre d'exécution de chaque ensemble de règles, puis Firewall Manager vous attribue les numéros lorsque vous enregistrez la politique. Vous pouvez définir jusqu'à 5 règles entrantes, réparties de quelque manière que ce soit entre la première et la dernière, et vous pouvez définir jusqu'à 5 règles sortantes.

   Pour obtenir des conseils sur la spécification des règles ACL réseau, consultez la section Ajouter et supprimer des règles ACL réseau dans le guide de l'utilisateur Amazon VPC.

   Les règles que vous définissez dans la politique Firewall Manager spécifient la configuration de règles minimale qu'une ACL réseau doit avoir pour être conforme à la politique ACL réseau. Par exemple, les règles entrantes d'une ACL réseau ne peuvent pas être conformes à la politique à moins qu'elles ne commencent par les premières règles entrantes de la politique, dans le même ordre que celui indiqué dans la stratégie. Pour plus d’informations, consultez Politiques ACL du réseau.
10. Pour Policy action (Action de stratégie), choisissez Identify resources that don’t comply with the policy rules, but don’t auto remediate (Identifier les ressources qui ne sont pas conformes aux règles de stratégie, mais ne pas effectuer une résolution automatique).
11. Choisissez Suivant.
12. Comptes AWS concerné par cette politique vous permet de réduire le champ d'application de votre politique en spécifiant les comptes à inclure ou à exclure. Pour ce didacticiel, choisissez Include all accounts under my organization (Inclure tous les comptes de mon organisation).

    Le type de ressource pour une politique ACL réseau est toujours sous-réseau.
13. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.

14. Choisissez Suivant.
15. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
16. Choisissez Suivant.
17. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Vérifiez que Policy action (Action de stratégie) est défini sur Identify resources that don't comply with the policy rules, but don't auto remediate (Identifier les ressources qui ne sont pas conformes aux règles de stratégie, mais ne pas effectuer une résolution automatique). Cela vous permet de passer en revue les modifications que votre politique apporterait avant de les activer.
18. Lorsque vous êtes satisfait de la politique, choisissez Créer une politique.

    Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique
19. Lorsque vous avez terminé votre exploration, si vous ne souhaitez pas conserver la politique que vous avez créée pour ce didacticiel, choisissez le nom de la politique, choisissez Supprimer, choisissez Nettoyer les ressources créées par cette politique. , puis choisissez Supprimer.

Pour plus d'informations sur les politiques ACL du réseau Firewall Manager, consultezPolitiques ACL du réseau.

Commencer à utiliser les AWS Firewall ManagerAWS Network Firewall politiques

AWS Firewall Manager Pour activer un pare-feu AWS Network Firewall au sein de votre organisation, effectuez les étapes suivantes dans l'ordre. Pour plus d'informations sur les politiques de Firewall Manager Network Firewall, consultezAWS Network Firewall politiques.

Rubriques

Étape 1 : Compléter les prérequis généraux

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez tous les prérequis avant de passer à l'étape suivante.

Étape 2 : créer un groupe de règles Network Firewall à utiliser dans votre politique

Pour suivre ce didacticiel, vous devez connaître AWS Network Firewall et savoir comment configurer ses groupes de règles et ses politiques de pare-feu.

Network Firewall doit comporter au moins un groupe de règles qui sera utilisé dans votre AWS Firewall Manager politique. Si vous n'avez pas encore créé de groupe de règles dans Network Firewall, faites-le maintenant. Pour plus d'informations sur l'utilisation de Network Firewall, consultez le manuel du AWS Network Firewall développeur.

Étape 3 : créer et appliquer une politique de Network Firewall

Après avoir rempli les conditions requises, vous créez une politique AWS Firewall Manager Network Firewall. Une politique de Network Firewall fournit un AWS Network Firewall pare-feu contrôlé de manière centralisée pour AWS l'ensemble de votre organisation. Il définit également les ressources Comptes AWS et les ressources auxquelles le pare-feu s'applique.

Pour plus d'informations sur la façon dont Firewall Manager gère vos politiques de Network Firewall, consultezAWS Network Firewall politiques.

Pour créer une politique de Firewall Manager Network Firewall (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Si vous ne remplissez pas les conditions requises, la console affiche des instructions sur la manière de résoudre les problèmes éventuels. Suivez les instructions, puis revenez à cette étape pour créer une politique Network Firewall.
4. Choisissez Créer une politique de sécurité.
5. Pour Policy type (Type de stratégie), choisissez AWS Network Firewall.
6. Pour Région, choisissez un Région AWS.
7. Choisissez Suivant.
8. Dans Nom de la politique, entrez un nom descriptif.
9. La configuration de la politique vous permet de définir la politique de pare-feu. Il s'agit du même processus que celui que vous utilisez dans la AWS Network Firewall console. Vous ajoutez les groupes de règles que vous souhaitez utiliser dans votre politique et vous fournissez les actions apatrides par défaut. Pour ce didacticiel, configurez cette politique comme vous le feriez pour une politique de pare-feu dans Network Firewall.

   > **Note**
   >
   > La correction automatique s'effectue automatiquement pour les politiques de AWS Firewall Manager Network Firewall. Vous ne verrez donc pas d'option vous permettant de ne pas procéder à la correction automatique ici.

10. Choisissez Suivant.
11. Pour les points de terminaison du pare-feu, sélectionnez Plusieurs points de terminaison du pare-feu. Cette option assure la haute disponibilité de votre pare-feu. Lorsque vous créez la

politique, Firewall Manager crée un sous-réseau de pare-feu dans chaque zone de disponibilité où vous devez protéger des sous-réseaux publics.

12. Pour la configuration des AWS Network Firewall itinéraires, choisissez Monitor pour que Firewall Manager surveille vos VPC pour détecter les violations de configuration des itinéraires et vous alerte avec des suggestions de mesures correctives pour vous aider à mettre les itinéraires en conformité. Si vous ne souhaitez pas que vos configurations d'itinéraires soient surveillées par Firewall Manager et que vous ne receviez pas ces alertes, choisissez Off.

> **Note**
>
> La surveillance vous fournit des informations sur les ressources non conformes dues à une configuration de route défectueuse et suggère des actions correctives à partir de l'API Firewall Manager`GetViolationDetails`. Par exemple, Network Firewall vous alerte si le trafic n'est pas acheminé via les points de terminaison du pare-feu créés par votre politique.

> **Warning**
>
> Si vous choisissez Monitor, vous ne pourrez pas le remplacer par Off à l'avenir pour la même politique. Vous devez créer une nouvelle politique.

13. Pour Type de trafic, sélectionnez Ajouter à la politique de pare-feu pour acheminer le trafic via la passerelle Internet.
14. Comptes AWS concerné par cette politique vous permet de réduire le champ d'application de votre politique en spécifiant les comptes à inclure ou à exclure. Pour ce didacticiel, choisissez Include all accounts under my organization (Inclure tous les comptes de mon organisation).

    Le type de ressource pour une politique Network Firewall est toujours VPC.
15. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.

16. Choisissez Suivant.
17. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
18. Choisissez Suivant.
19. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Vérifiez que Policy action (Action de stratégie) est défini sur Identify resources that don't comply with the policy rules, but don't auto remediate (Identifier les ressources qui ne sont pas conformes aux règles de stratégie, mais ne pas effectuer une résolution automatique). Cela vous permet de passer en revue les modifications que votre politique apporterait avant de les activer.
20. Lorsque vous êtes satisfait de la politique, choisissez Créer une politique.

    Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique
21. Lorsque vous avez terminé votre exploration, si vous ne souhaitez pas conserver la politique que vous avez créée pour ce didacticiel, choisissez le nom de la politique, choisissez Supprimer, choisissez Nettoyer les ressources créées par cette politique. , puis choisissez Supprimer.

Pour plus d'informations sur les politiques de Firewall Manager Network Firewall, consultezAWS Network Firewall politiques.

Commencer à utiliser les politiques de pare-feu AWS Firewall Manager DNS

AWS Firewall Manager Pour activer le pare-feu DNS Amazon Route 53 Resolver au sein de votre organisation, effectuez les étapes suivantes dans l'ordre. Pour plus d'informations sur les politiques de pare-feu DNS de Firewall Manager, consultezPolitiques de pare-feu DNS d'Amazon Route 53 Resolver.

Rubriques

Étape 1 : Compléter les prérequis généraux

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez tous les prérequis avant de passer à l'étape suivante.

Étape 2 : Créez les groupes de règles de votre pare-feu DNS à utiliser dans votre politique

Pour suivre ce didacticiel, vous devez connaître le pare-feu DNS Amazon Route 53 Resolver et savoir comment configurer ses groupes de règles.

Vous devez avoir au moins un groupe de règles dans le pare-feu DNS qui sera utilisé dans votre AWS Firewall Manager politique. Si vous n'avez pas encore créé de groupe de règles dans le pare-feu DNS, faites-le maintenant. Pour plus d'informations sur l'utilisation du pare-feu DNS, consultez le pare-feu DNS Amazon Route 53 Resolver dans le guide du développeur Amazon Route 53.

Étape 3 : créer et appliquer une politique de pare-feu DNS

Après avoir rempli les conditions requises, vous créez une politique de pare-feu AWS Firewall Manager DNS. Une politique de pare-feu DNS fournit un ensemble d'associations de groupes de règles de pare-feu DNS contrôlées de manière centralisée pour AWS l'ensemble de votre organisation. Il définit également les ressources Comptes AWS et les ressources auxquelles le pare-feu s'applique.

Pour plus d'informations sur la façon dont Firewall Manager gère vos associations de groupes de règles de pare-feu DNS, consultezPolitiques de pare-feu DNS d'Amazon Route 53 Resolver.

Pour créer une politique de pare-feu DNS Firewall Manager (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.
2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Si vous ne remplissez pas les conditions requises, la console affiche des instructions sur la manière de résoudre les problèmes éventuels. Suivez les instructions, puis revenez à cette étape pour créer une politique de pare-feu DNS.
4. Choisissez Créer une politique de sécurité.
5. Pour le type de politique, choisissez Amazon Route 53 Resolver DNS Firewall.
6. Pour Région, choisissez un Région AWS.
7. Choisissez Suivant.
8. Dans Nom de la politique, entrez un nom descriptif.
9. La configuration des politiques vous permet de définir les associations de groupes de règles du pare-feu DNS que vous souhaitez gérer à partir de Firewall Manager. Vous ajoutez les groupes de règles que vous souhaitez utiliser dans votre politique. Vous pouvez définir une association à évaluer en premier pour vos VPC et une autre à évaluer en dernier. Pour ce didacticiel, ajoutez une ou deux associations de groupes de règles, en fonction de vos besoins.
10. Choisissez Suivant.
11. Comptes AWS concerné par cette politique vous permet de réduire le champ d'application de votre politique en spécifiant les comptes à inclure ou à exclure. Pour ce didacticiel, choisissez Include all accounts under my organization (Inclure tous les comptes de mon organisation).

    Le type de ressource pour une politique de pare-feu DNS est toujours VPC.
12. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.

13. Choisissez Suivant.
14. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
15. Choisissez Suivant.
16. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Vérifiez que Policy action (Action de stratégie) est défini sur Identify resources that don't comply with the policy rules, but don't auto remediate (Identifier les ressources qui ne sont pas conformes aux règles de stratégie, mais ne pas effectuer une résolution automatique). Cela vous permet de passer en revue les modifications que votre politique apporterait avant de les activer.
17. Lorsque vous êtes satisfait de la politique, choisissez Créer une politique.

    Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique
18. Lorsque vous avez terminé votre exploration, si vous ne souhaitez pas conserver la politique que vous avez créée pour ce didacticiel, choisissez le nom de la politique, choisissez Supprimer, choisissez Nettoyer les ressources créées par cette politique. , puis choisissez Supprimer.

Pour plus d'informations sur les politiques de pare-feu DNS de Firewall Manager, consultezPolitiques de pare-feu DNS d'Amazon Route 53 Resolver.

Commencer à utiliser les AWS Firewall Manager politiques de pare-feu de nouvelle génération de Palo Alto Networks Cloud

AWS Firewall Manager Pour activer les politiques de pare-feu de nouvelle génération (NGFW) de Palo Alto Networks Cloud, effectuez les étapes suivantes dans l'ordre. Pour plus d'informations sur les politiques NGFW de Palo Alto Networks Cloud, consultez. Politiques NGFW de Palo Alto Networks Cloud

Rubriques

Étape 1 : Compléter les prérequis généraux

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez tous les prérequis avant de passer à l'étape suivante.

Étape 2 : remplir les conditions préalables à la politique NGFW de Palo Alto Networks Cloud

Vous devez effectuer quelques étapes obligatoires supplémentaires pour utiliser les politiques NGFW de Palo Alto Networks Cloud. Ces étapes sont décrites dans Conditions préalables à la politique de pare-feu de nouvelle génération de Palo Alto Networks Cloud. Complétez tous les prérequis avant de passer à l'étape suivante.

Étape 3 : créer et appliquer une politique NGFW de Palo Alto Networks Cloud

Une fois les prérequis remplis, vous créez une politique AWS Firewall Manager Palo Alto Networks Cloud NGFW.

Pour plus d'informations sur les politiques de Firewall Manager pour Palo Alto Networks Cloud NGFW, consultez. Politiques NGFW de Palo Alto Networks Cloud

Pour créer une politique Firewall Manager pour Palo Alto Networks Cloud NGFW (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour le type de politique, choisissez Palo Alto Networks Cloud NGFW. Si vous n'êtes pas encore abonné au service Palo Alto Networks Cloud NGFW sur AWS Marketplace, vous devez d'abord le faire. Pour vous abonner à la AWS Marketplace, choisissez View AWS Marketplace details.
5. Pour le modèle de déploiement, choisissez le modèle distribué ou le modèle centralisé.
   Le modèle de déploiement détermine la manière dont Firewall Manager gère les points de terminaison pour la politique. Avec le modèle distribué, Firewall Manager gère les points de terminaison du pare-feu dans chaque VPC relevant du champ d'application des politiques. Avec le modèle centralisé, Firewall Manager gère un point de terminaison unique dans un VPC d'inspection.
6. Pour Région, choisissez un Région AWS. Pour protéger les ressources de plusieurs régions, vous devez créer des politiques distinctes pour chaque région.
7. Choisissez Suivant.
8. Dans Nom de la politique, entrez un nom descriptif.
9. Dans la configuration de la politique, choisissez la politique de pare-feu Palo Alto Networks Cloud NGFW à associer à cette politique. La liste des politiques de pare-feu Palo Alto Networks Cloud NGFW contient toutes les politiques de pare-feu Palo Alto Networks Cloud NGFW associées à votre client Palo Alto Networks Cloud NGFW. Pour plus d'informations sur la création et la gestion des politiques de pare-feu NGFW de Palo Alto Networks Cloud, consultez la AWS Firewall Manager rubrique Deploy Palo Alto Networks Cloud NGFW pour AWS le guide de déploiement. AWS
10. Pour la journalisation NGFW dans le cloud de Palo Alto Networks, vous pouvez éventuellement choisir le ou les types de journaux NGFW de Palo Alto Networks Cloud à enregistrer

conformément à votre politique. Pour plus d'informations sur les types de journaux NGFW de Palo Alto Networks Cloud, voir Configurer la journalisation pour Palo Alto Networks Cloud NGFW on AWS dans le guide de déploiement de Palo Alto Networks Cloud NGFW. AWS

Pour la destination des journaux, spécifiez à quel moment Firewall Manager doit écrire les journaux.

11. Choisissez Suivant.
12. Sous Configurer un point de terminaison de pare-feu tiers, effectuez l'une des opérations suivantes, selon que vous utilisez le modèle de déploiement distribué ou centralisé pour créer vos points de terminaison de pare-feu :

    - Si vous utilisez le modèle de déploiement distribué pour cette politique, sous Zones de disponibilité, sélectionnez les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu. Vous pouvez sélectionner des zones de disponibilité par nom de zone de disponibilité ou par ID de zone de disponibilité.
    - Si vous utilisez le modèle de déploiement centralisé pour cette politique, dans la configuration du point de AWS Firewall Manager terminaison sous Configuration du VPC d'inspection, entrez l'ID de AWS compte du propriétaire du VPC d'inspection et l'ID du VPC d'inspection.
        - Sous Zones de disponibilité, sélectionnez les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu. Vous pouvez sélectionner des zones de disponibilité par nom de zone de disponibilité ou par ID de zone de disponibilité.
13. Choisissez Suivant.
14. Pour le champ d'application de la politique, dans le cadre de Comptes AWS cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.
    - Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et

unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

Vous ne pouvez choisir qu'une des options.

Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.

Le type de ressource pour les politiques Network Firewall est VPC.

15. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.

16. Pour accorder un accès entre comptes, choisissez Télécharger le AWS CloudFormation modèle. Cela télécharge un AWS CloudFormation modèle que vous pouvez utiliser pour créer une AWS CloudFormation pile. Cette pile crée un AWS Identity and Access Management rôle qui accorde à Firewall Manager des autorisations inter-comptes pour gérer les ressources NGFW Cloud de Palo Alto Networks. Pour plus d'informations sur les piles, reportez-vous à la section Utilisation des piles dans le Guide de l'AWS CloudFormation utilisateur.
17. Choisissez Suivant.
18. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

19. Choisissez Suivant.
20. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Vérifiez que Policy action (Action de stratégie) est défini sur Identify resources that don't comply with the policy rules, but don't auto remediate (Identifier les ressources qui ne sont pas conformes aux règles de stratégie, mais ne pas effectuer une résolution automatique). Cela vous permet de passer en revue les modifications que votre politique apporterait avant de les activer.
21. Lorsque vous êtes satisfait de la politique, choisissez Créer une politique.

    Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

Pour plus d'informations sur les politiques NGFW du Firewall Manager Palo Alto Networks Cloud, consultez. Politiques NGFW de Palo Alto Networks Cloud

Commencer à utiliser les politiques de AWS Firewall Manager Fortigate CNF

Fortigate Cloud Native Firewall (CNF) as a Service est un service de pare-feu tiers que vous pouvez utiliser pour vos politiques. AWS Firewall Manager Avec Fortigate CNF for Firewall Manager, vous pouvez créer et déployer de manière centralisée des ressources et des ensembles de politiques Fortigate CNF sur tous vos comptes. AWS AWS Firewall Manager Pour activer les politiques Fortigate CNF, effectuez les étapes suivantes dans l'ordre. Pour plus d'informations sur les politiques de Fortigate CNF, consultez. Politiques de pare-feu natif du cloud (CNF) de Fortigate en tant que service

Rubriques

- Étape 1 : Compléter les prérequis généraux
- Étape 2 : remplir les conditions préalables à la politique Fortigate CNF
- Étape 3 : créer et appliquer une politique Fortigate CNF

Étape 1 : Compléter les prérequis généraux

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez tous les prérequis avant de passer à l'étape suivante.

Étape 2 : remplir les conditions préalables à la politique Fortigate CNF

Il existe des étapes obligatoires supplémentaires que vous devez suivre pour utiliser les politiques Fortigate CNF. Ces étapes sont décrites dans Conditions préalables à la politique Fortigate Cloud Native Firewall (CNF) en tant que service. Complétez tous les prérequis avant de passer à l'étape suivante.

Étape 3 : créer et appliquer une politique Fortigate CNF

Après avoir rempli les conditions requises, vous créez une politique AWS Firewall Manager Fortigate CNF.

Pour plus d'informations sur les politiques de Firewall Manager pour Fortigate CNF, consultez. Politiques de pare-feu natif du cloud (CNF) de Fortigate en tant que service

Pour créer une politique Firewall Manager pour Fortigate CNF (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour le type de politique, choisissez Fortigate CNF. Si vous n'êtes pas encore abonné au service Fortigate CNF sur le AWS Marketplace, vous devez d'abord le faire. Pour vous abonner à la AWS Marketplace, choisissez View AWS Marketplace details.

5. Pour le modèle de déploiement, choisissez le modèle distribué ou le modèle centralisé. Le modèle de déploiement détermine la manière dont Firewall Manager gère les points de terminaison pour la politique. Avec le modèle distribué, Firewall Manager gère les points de terminaison du pare-feu dans chaque VPC relevant du champ d'application des politiques. Avec le modèle centralisé, Firewall Manager gère un point de terminaison unique dans un VPC d'inspection.
6. Pour Région, choisissez un Région AWS. Pour protéger les ressources de plusieurs régions, vous devez créer des politiques distinctes pour chaque région.
7. Choisissez Suivant.
8.
9. Dans la configuration de la politique, choisissez la politique de pare-feu Fortigate CNF à associer à cette politique. La liste des politiques de pare-feu Fortigate CNF contient toutes les politiques de pare-feu Fortigate CNF associées à votre client Fortigate CNF. Pour plus d'informations sur la création et la gestion des politiques de pare-feu Fortigate CNF, consultez la documentation de Fortigate CNF.
10. Choisissez Suivant.
11. Sous Configurer un point de terminaison de pare-feu tiers, effectuez l'une des opérations suivantes, selon que vous utilisez le modèle de déploiement distribué ou centralisé pour créer vos points de terminaison de pare-feu :

    - Si vous utilisez le modèle de déploiement distribué pour cette politique, sous Zones de disponibilité, sélectionnez les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu. Vous pouvez sélectionner des zones de disponibilité par nom de zone de disponibilité ou par ID de zone de disponibilité.
    - Si vous utilisez le modèle de déploiement centralisé pour cette politique, dans la configuration du point de AWS Firewall Manager terminaison sous Configuration du VPC d'inspection, entrez l'ID de AWS compte du propriétaire du VPC d'inspection et l'ID du VPC d'inspection.
        - Sous Zones de disponibilité, sélectionnez les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu. Vous pouvez sélectionner des zones de disponibilité par nom de zone de disponibilité ou par ID de zone de disponibilité.
12. Choisissez Suivant.
13. Pour le champ d'application de la politique, dans le cadre de Comptes AWS cette politique s'applique à, choisissez l'option suivante :

- Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
- Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.
- Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

Vous ne pouvez choisir qu'une des options.

Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.

Le type de ressource pour les politiques Fortigate CNF est VPC.

14. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ».

Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.

15. Pour accorder un accès entre comptes, choisissez Télécharger le AWS CloudFormation modèle. Cela télécharge un AWS CloudFormation modèle que vous pouvez utiliser pour créer une AWS CloudFormation pile. Cette pile crée un AWS Identity and Access Management rôle qui accorde à Firewall Manager des autorisations entre comptes pour gérer les ressources Fortigate CNF. Pour plus d'informations sur les piles, reportez-vous à la section Utilisation des piles dans le Guide de l'AWS CloudFormation utilisateur. Pour créer une pile, vous aurez besoin de l'identifiant de compte du portail Fortigate CNF.
16. Choisissez Suivant.
17. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
18. Choisissez Suivant.
19. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Vérifiez que Policy action (Action de stratégie) est défini sur Identify resources that don't comply with the policy rules, but don't auto remediate (Identifier les ressources qui ne sont pas conformes aux règles de stratégie, mais ne pas effectuer une résolution automatique). Cela vous permet de passer en revue les modifications que votre politique apporterait avant de les activer.
20. Lorsque vous êtes satisfait de la politique, choisissez Créer une politique.

    Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

Pour plus d'informations sur les politiques CNF de Firewall Manager Fortigate, consultez. Politiques de pare-feu natif du cloud (CNF) de Fortigate en tant que service

Travailler avec les AWS Firewall Manager politiques

AWS Firewall Manager fournit les types de politiques suivants. Pour chaque type de politique, vous définissez les éléments suivants :

- AWS WAFpolitique : Firewall Manager prend en charge AWS WAF les politiques AWS WAF classiques. Pour les deux versions, vous définissez les ressources qui seront protégées par la stratégie.
  - Le type de AWS WAF politique nécessite des ensembles de groupes de règles à exécuter en premier et en dernier dans l'ACL Web. Ensuite, dans les comptes auxquels vous appliquez l'ACL Web, le propriétaire du compte peut ajouter des règles et des groupes de règles à exécuter entre les deux ensembles.
  - Le type de politique AWS WAF classique nécessite l'exécution d'un seul groupe de règles dans l'ACL Web.
- Politique Shield Advanced : ce type de politique applique les protections Shield Advanced à l'ensemble de votre organisation pour les types de ressources que vous spécifiez.
- Politique des groupes de sécurité Amazon VPC : ce type de politique vous permet de contrôler les groupes de sécurité utilisés au sein de votre organisation et d'appliquer un ensemble de règles de base au sein de votre organisation.
- Politique relative à la liste de contrôle d'accès réseau (ACL) Amazon VPC : ce type de politique vous permet de contrôler les listes de contrôle d'accès réseau utilisées dans l'ensemble de votre organisation et d'appliquer un ensemble de référence d'ACL réseau au sein de votre organisation.
- Stratégie Network Firewall : ce type de politique applique AWS Network Firewall une protection aux VPC de votre entreprise.
- Politique de pare-feu DNS d'Amazon Route 53 Resolver : cette politique applique les protections du pare-feu DNS aux VPC de votre entreprise.
- Politique de pare-feu tiers : ce type de politique applique des protections de pare-feu tierces. Les pare-feux tiers sont disponibles par abonnement via la console AWS Marketplace sur AWS Marketplace.
  - Politique NGFW cloud de Palo Alto Networks — Ce type de politique applique les protections du pare-feu de nouvelle génération (NGFW) de Palo Alto Networks Cloud et les règles NGFW de Palo Alto Networks Cloud aux VPC de votre organisation.
  - Politique Fortigate Cloud Native Firewall (CNF) en tant que service — Ce type de politique applique les protections Fortigate Cloud Native Firewall (CNF) en tant que service. Fortigate CNF est une solution centrée sur le cloud qui bloque les menaces Zero-Day et sécurise

les infrastructures cloud grâce à une prévention avancée des menaces, à des pare-feux d'applications Web (WAF) intelligents et à une protection des API de pointe.

Une politique Firewall Manager est spécifique à chaque type de stratégie. Si vous souhaitez appliquer plusieurs types de stratégie sur les comptes, vous pouvez créer plusieurs stratégies. Vous pouvez créer plusieurs stratégies pour chaque type.

Si vous ajoutez un nouveau compte à une organisation que vous avez créée avec AWS Organizations, Firewall Manager applique automatiquement la politique aux ressources de ce compte qui sont couvertes par cette politique.

Paramètres généraux des AWS Firewall Manager politiques

AWS Firewall Manager les politiques gérées ont des paramètres et des comportements communs. Pour tous, vous spécifiez un nom et définissez la portée de la politique, et vous pouvez utiliser le balisage des ressources pour contrôler la portée de la politique. Vous pouvez choisir d'afficher les comptes et les ressources non conformes sans prendre de mesures correctives ou de corriger automatiquement les ressources non conformes.

Pour plus d'informations sur le champ d'application de la politique, consultezAWS Firewall Manager portée de la politique.

Création d'une AWS Firewall Manager politique

Les étapes de création d'une stratégie varient selon le type de stratégie. Assurez-vous d'utiliser la procédure correspondant au type de stratégie dont vous avez besoin.

> **Important**
>
> AWS Firewall Manager ne prend pas en charge Amazon Route 53 ou AWS Global Accelerator. Si vous souhaitez protéger ces ressources avec Shield Advanced, vous ne pouvez pas utiliser une politique de Firewall Manager. Au lieu de cela, suivez les instructions de Ajouter AWS Shield Advanced une protection aux AWS ressources.

Rubriques

- Création d'une AWS Firewall Manager politique pour AWS WAF

- Création d'une AWS Firewall Manager politique pour AWS WAF Classic
- Création d'une AWS Firewall Manager politique pour AWS Shield Advanced
- Création d'une stratégie de groupe de sécurité AWS Firewall Manager commune
- Création d'une stratégie de groupe de sécurité d'audit de contenu AWS Firewall Manager
- Création d'une stratégie de groupe de sécurité d'audit d'utilisation AWS Firewall Manager
- Création d'une politique ACL AWS Firewall Manager réseau
- Création d'une AWS Firewall Manager politique pour AWS Network Firewall
- Création d'une AWS Firewall Manager politique pour le pare-feu DNS Amazon Route 53 Resolver
- Création d'une AWS Firewall Manager politique pour Palo Alto Networks Cloud NGFW
- Création d'une AWS Firewall Manager politique pour Fortigate Cloud Native Firewall (CNF) en tant que service

Création d'une AWS Firewall Manager politique pour AWS WAF

Dans une AWS WAF politique de Firewall Manager, vous pouvez utiliser des groupes de règles gérés, AWS que AWS Marketplace les vendeurs créent et gèrent pour vous. Vous pouvez également créer et utiliser vos propres groupes de règles. Pour de plus amples informations sur les groupes de correctifs, veuillez consulter AWS WAF groupes de règles.

Si vous souhaitez utiliser vos propres groupes de règles, créez-les avant de créer votre AWS WAF politique Firewall Manager. Pour de plus amples informations, consultez Gestion de vos propres groupes de règles. Pour utiliser une règle personnalisée individuelle, vous devez définir votre propre groupe de règles, définir votre règle à l'intérieur de celui-ci, puis utiliser le groupe de règles dans votre stratégie.

Pour plus d'informations sur les AWS WAF politiques de Firewall Manager, consultezAWS WAF politiques.

Pour créer une politique Firewall Manager pour AWS WAF (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

> **Note**
>
> Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour Policy type (Type de stratégie), choisissez AWS WAF.
5. Pour Région, choisissez un Région AWS. Pour protéger les CloudFront distributions Amazon, choisissez Global.

   Pour protéger les ressources dans plusieurs régions (autres que les CloudFront distributions), vous devez créer des politiques Firewall Manager distinctes pour chaque région.
6. Choisissez Suivant.
7. Dans Nom de la politique, entrez un nom descriptif. Firewall Manager inclut le nom de la politique dans les noms des ACL Web qu'il gère. Les noms des ACL Web sont `FMManagedWebACLV2-` suivis du nom de la politique que vous entrez ici et de l'horodatage de création des ACL Web, en millisecondes UTC. - Par exemple, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.
8. Pour l'inspection du corps d'une demande Web, modifiez éventuellement la limite de taille du corps. Pour plus d'informations sur les limites de taille pour l'inspection des carrosseries, y compris les considérations tarifaires, consultez Gestion des limites de taille des organismes inspectés le guide du AWS WAF développeur.
9. Sous Règles de politique, ajoutez les groupes de règles que vous AWS WAF souhaitez évaluer en premier et en dernier dans l'ACL Web. Pour utiliser le contrôle de version de groupes de règles AWS WAF gérés, activez l'option Activer le contrôle de version. Les gestionnaires de comptes individuels peuvent ajouter des règles et des groupes de règles entre vos premiers groupes de règles et vos derniers groupes de règles. Pour plus d'informations sur l'utilisation de groupes de AWS WAF règles dans les politiques de Firewall Manager pour AWS WAF, consultezAWS WAF politiques.

   (Facultatif) Pour personnaliser la façon dont votre ACL Web utilise le groupe de règles, choisissez Modifier. Les paramètres de personnalisation courants sont les suivants :

   - Pour les groupes de règles gérés, remplacez les actions des règles pour certaines ou toutes les règles. Si vous ne définissez pas d'action de remplacement pour une règle, l'évaluation

utilise l'action de règle définie au sein du groupe de règles. Pour plus d'informations sur cette option, consultez Options de dérogation aux actions pour les groupes de règles le guide du AWS WAF développeur.

- Certains groupes de règles gérés nécessitent que vous fournissiez une configuration supplémentaire. Consultez la documentation de votre fournisseur de groupes de règles gérés. Pour obtenir des informations spécifiques aux groupes de règles AWS gérées, consultez AWS Règles gérées pour AWS WAF le guide du AWS WAF développeur.

Lorsque vous avez terminé de définir vos paramètres, choisissez Enregistrer la règle.

10. Définissez l'action par défaut pour la liste ACL web. Il s'agit de l'action AWS entreprise par le WAF lorsqu'une requête Web ne correspond à aucune des règles de l'ACL Web. Vous pouvez ajouter des en-têtes personnalisés avec l'action Autoriser ou des réponses personnalisées pour l'action Bloquer. Pour plus d'informations sur les actions ACL Web par défaut, consultezL'action par défaut de l'ACL Web. Pour plus d'informations sur la définition de requêtes Web et de réponses personnalisées, consultezDemandes et réponses Web personnalisées dans AWS WAF.
11. Pour la configuration de la journalisation, choisissez Activer la journalisation pour activer la journalisation. La journalisation fournit des informations détaillées sur le trafic analysé par votre ACL Web. Choisissez la destination de journalisation, puis choisissez la destination de journalisation que vous avez configurée. Vous devez choisir une destination de journalisation dont le nom commence par`aws-waf-logs-`. Pour plus d'informations sur la configuration d'une destination de AWS WAF journalisation, consultezConfiguration de la journalisation pour une AWS WAF politique.
12. (Facultatif) Si vous ne souhaitez pas que certains champs et leurs valeurs soient inclus dans les journaux, censurez ces champs. Choisissez le champ à censurer, puis choisissez Ajouter. Répétez si nécessaire pour censurer des champs supplémentaires. Les champs censurés apparaîtront en tant que `REDACTED` dans les journaux. Par exemple, si vous supprimez le champ URI, le champ URI des journaux sera`REDACTED`.
13. (Facultatif) Si vous ne souhaitez pas envoyer toutes les demandes aux journaux, ajoutez vos critères de filtrage et votre comportement. Sous Filtrer les journaux, pour chaque filtre que vous souhaitez appliquer, choisissez Ajouter un filtre, puis choisissez vos critères de filtrage et indiquez si vous souhaitez conserver ou supprimer les demandes correspondant à ces critères. Lorsque vous avez fini d'ajouter des filtres, modifiez si nécessaire le comportement de journalisation par défaut. Pour plus d'informations, consultez Configuration de la journalisation des ACL Web dans le Guide du développeur AWS WAF .

14. Vous pouvez définir une liste de domaines de jetons pour permettre le partage de jetons entre les applications protégées. Les jetons sont utilisés par les Challenge actions CAPTCHA et par les SDK d'intégration d'applications que vous implémentez lorsque vous utilisez les groupes de règles AWS gérées pour le contrôle des AWS WAF fraudes, la prévention du rachat de compte (ATP) et le contrôle des AWS WAF bots.

    Les suffixes publics ne sont pas autorisés. Par exemple, vous ne pouvez pas utiliser `gov.au` ou `co.uk` comme domaine de jetons.

    Par défaut, AWS WAF accepte les jetons uniquement pour le domaine de la ressource protégée. Si vous ajoutez des domaines de jetons dans cette liste, AWS WAF les jetons sont acceptés pour tous les domaines de la liste et pour le domaine de la ressource associée. Pour plus d'informations, consultez AWS WAF configuration de la liste de domaines du jeton ACL Web dans le Guide du développeur AWS WAF .

    Vous ne pouvez modifier le CAPTCHA de l'ACL Web et contester les temps d'immunité que lorsque vous modifiez une ACL Web existante. Vous trouverez ces paramètres sur la page de détails de la politique de Firewall Manager. Pour plus d'informations sur ces paramètres, consultez Expiration de l'horodatage : durée d'immunité des AWS WAF jetons. Si vous mettez à jour les paramètres de configuration d'association, de CAPTCHA, de défi ou de liste de domaines dans une politique existante, Firewall Manager remplacera vos ACL Web locales par les nouvelles valeurs. Toutefois, si vous ne mettez pas à jour les paramètres de configuration d'association, de CAPTCHA, de défi ou de liste de domaines de jetons de la politique, les valeurs de vos ACL Web locales resteront inchangées. Pour plus d'informations sur cette option, consultez CAPTCHAet Challenge dans AWS WAF le guide du AWS WAF développeur.

15. Dans la section Gestion des ACL Web, si vous souhaitez que Firewall Manager gère les ACL Web non associées, activez l'option Gérer les ACL Web non associées. Avec cette option, Firewall Manager crée des ACL Web dans les comptes relevant du champ d'application de la politique uniquement si les ACL Web sont destinées à être utilisées par au moins une ressource. À tout moment, si un compte entre dans le champ d'application de la politique, Firewall Manager crée automatiquement une ACL Web dans le compte si au moins une ressource utilise l'ACL Web. Lorsque cette option est activée, Firewall Manager effectue un nettoyage unique des ACL Web non associées dans votre compte. Le processus de nettoyage peut prendre plusieurs heures. Si une ressource quitte le champ d'application de la politique après que Firewall Manager a créé une ACL Web, Firewall Manager dissocie la ressource de l'ACL Web, mais ne nettoie pas l'ACL Web non associée. Firewall Manager nettoie les ACL Web non associées

uniquement lorsque vous activez pour la première fois la gestion des ACL Web non associées dans une politique.

16. Pour l'action stratégique, si vous souhaitez créer une ACL Web dans chaque compte applicable au sein de l'organisation, mais ne pas encore appliquer l'ACL Web à aucune ressource, choisissez Identifier les ressources qui ne sont pas conformes aux règles de politique, mais ne corrigez pas automatiquement et ne choisissez pas Gérer les ACL Web non associées. Vous pourrez modifier ces options ultérieurement.

    Si vous souhaitez plutôt appliquer automatiquement la stratégie aux ressources concernées existantes, choisissez Auto remediate any noncompliant resources (Corriger automatiquement les ressources non conformes). Si Gérer les ACL Web non associées est désactivée, l'option Corriger automatiquement les ressources non conformes crée une ACL Web dans chaque compte applicable au sein de l'organisation et associe l'ACL Web aux ressources des comptes. Si Gérer les ACL Web non associées est activée, l'option Corriger automatiquement les ressources non conformes crée et associe uniquement une ACL Web aux comptes dont les ressources peuvent être associées à l'ACL Web.

    Lorsque vous choisissez Corriger automatiquement les ressources non conformes, vous pouvez également choisir de supprimer les associations d'ACL Web existantes des ressources incluses, pour les ACL Web qui ne sont pas gérées par une autre politique active de Firewall Manager. Si vous choisissez cette option, Firewall Manager associe d'abord l'ACL Web de la politique aux ressources, puis supprime les associations précédentes. Si une ressource est associée à une autre ACL Web gérée par une autre politique active de Firewall Manager, ce choix n'affecte pas cette association.

17. Choisissez Suivant.

18. Pour Comptes AWS que cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

- Si vous souhaitez appliquer la stratégie à tous les comptes ou unités d'organisation AWS Organizations à l'exception d'un ensemble spécifique, choisissez Exclude the specified accounts and organizational units, and include all others (Exclure les comptes et unités d'organisation spécifiés et inclure tous les autres), puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

Vous ne pouvez choisir qu'une des options.

Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.

19. Pour Resource type (Type de ressource), choisissez les types de ressources que vous souhaitez protéger.
20. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.
21. Choisissez Suivant.
22. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
23. Choisissez Suivant.

24. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Lorsque vous êtes satisfait de la politique, choisissez Créer une politique. Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

Création d'une AWS Firewall Manager politique pour AWS WAF Classic

Pour créer une politique Firewall Manager pour AWS WAF Classic (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour Type de stratégie, choisissez AWS WAF Classic.
5. Si vous avez déjà créé le groupe de règles AWS WAF classique que vous souhaitez ajouter à la politique, choisissez Créer une AWS Firewall Manager politique et ajoutez des groupes de règles existants. Si vous souhaitez créer un nouveau groupe de règles, choisissez Create a Firewall Manager policy et ajoutez un nouveau groupe de règles.
6. Pour Région, choisissez un Région AWS. Pour protéger les CloudFront ressources Amazon, choisissez Global.

Pour protéger les ressources de plusieurs régions (autres que les CloudFront ressources), vous devez créer des politiques Firewall Manager distinctes pour chaque région.

7. Choisissez Suivant.
8. Si vous créez un groupe de règles, suivez les instructions fournies dans Création d'un groupe de règles AWS WAF classique. Une fois que vous avez créé le groupe de règles, poursuivez avec les étapes suivantes.
9. Entrez un nom de stratégie.
10. Si vous ajoutez un groupe de règles prédéfini, utilisez le menu déroulant pour sélectionner le groupe de règles à ajouter, puis choisissez Add rule group (Ajouter le groupe de règles).
11. Une stratégie a deux actions possibles : Action définie par un groupe de règles et Nombre. Si vous souhaitez tester la stratégie et le groupe de règles, définissez l'action sur Nombre. Cette action remplace toute action de blocage spécifiée par le groupe de règles contenu dans la stratégie. Autrement dit, si l'action de la stratégie est définie sur Nombre, ces demandes sont uniquement comptabilisées et ne sont pas bloquées. À l'inverse, si vous définissez l'action de la stratégie sur Action set by rule group (Action définie par le groupe de règles), les actions du groupe de règles de la stratégie sont utilisées. Choisissez l'action appropriée.
12. Choisissez Suivant.
13. Pour Comptes AWS que cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.
    - Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

Vous ne pouvez choisir qu'une des options.

Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.

14. Choisissez le type de ressource que vous voulez protéger.
15. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.
16. Si vous souhaitez appliquer automatiquement la stratégie à des ressources existantes, choisissez Créer et appliquer cette stratégie à des ressources existantes et nouvelles.

    Cette option crée une liste ACL web dans chaque compte applicable dans une organisation AWS et l'associe aux ressources des comptes. Cette option applique également la stratégie à toutes les nouvelles ressources qui correspondent aux précédents critères (type de ressource et balises). Sinon, si vous choisissez Créer une stratégie, mais ne pas l'appliquer aux ressources existantes ou nouvelles, Firewall Manager crée une liste ACL web dans chaque compte applicable de l'organisation, mais ne l'applique pas aux ressources. Vous devrez appliquer la stratégie aux ressources ultérieurement. Choisissez l'option appropriée.
17. Dans Replace existing associated web ACLs (Remplacer les listes ACL web associées existantes), vous pouvez choisir de supprimer toutes les associations ACL web actuellement définies pour les ressources concernées, puis de les remplacer par des associations aux listes ACL web que vous créez avec cette stratégie. Par défaut, Firewall Manager ne supprime pas les

associations ACL Web existantes avant d'en ajouter de nouvelles. Si vous souhaitez supprimer les associations existantes, choisissez cette option.

18. Choisissez Suivant.
19. Passez en revue la nouvelle stratégie. Pour effectuer des modifications, sélectionnez Modifier. Lorsque vous êtes satisfait de la stratégie, choisissez Créer et appliquer une stratégie.

Création d'une AWS Firewall Manager politique pour AWS Shield Advanced

Pour créer une politique Firewall Manager pour Shield Advanced (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour le type de politique, choisissez Shield Advanced.

   Pour créer une politique Shield Advanced, vous devez être abonné à Shield Advanced. Si vous n'êtes pas abonné, vous êtes invité à le faire. Pour plus d'informations sur le coût de l'abonnement, consultez la section AWS Shield Advanced Tarification.
5. Pour Région, choisissez un Région AWS. Pour protéger les CloudFront distributions Amazon, choisissez Global.

   Pour les choix de régions autres que Global, afin de protéger les ressources de plusieurs régions, vous devez créer une politique Firewall Manager distincte pour chaque région.
6. Choisissez Suivant.
7. Dans Nom, entrez un nom descriptif.
8. Pour les politiques régionales mondiales uniquement, vous pouvez choisir si vous souhaitez gérer l'atténuation automatique des attaques DDoS au niveau de la couche d'application Shield

Advanced. Pour plus d'informations sur cette fonctionnalité Shield Advanced, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

Vous pouvez choisir d'activer ou de désactiver l'atténuation automatique, ou de l'ignorer. Si vous choisissez de l'ignorer, Firewall Manager ne gère aucune atténuation automatique pour les protections Shield Advanced. Pour plus d'informations sur ces options de stratégie, consultezAtténuation automatique des attaques DDoS au niveau de.

9. Dans la section Gestion des ACL Web, si vous souhaitez que Firewall Manager gère les ACL Web non associées, activez l'option Gérer les ACL Web non associées. Avec cette option, Firewall Manager crée des ACL Web dans les comptes relevant du champ d'application de la politique uniquement si les ACL Web sont destinées à être utilisées par au moins une ressource. À tout moment, si un compte entre dans le champ d'application de la politique, Firewall Manager crée automatiquement une ACL Web dans le compte si au moins une ressource utilise l'ACL Web. Lorsque cette option est activée, Firewall Manager effectue un nettoyage unique des ACL Web non associées dans votre compte. Le processus de nettoyage peut prendre plusieurs heures. Si une ressource quitte le champ d'application de la politique après que Firewall Manager ait créé une ACL Web, Firewall Manager ne dissociera pas la ressource de l'ACL Web. Pour inclure l'ACL Web dans le nettoyage unique, vous devez d'abord dissocier manuellement les ressources de l'ACL Web, puis activer Gérer les ACL Web non associées.
10. Pour ce qui est de l'action stratégique, nous recommandons de créer la politique avec l'option qui ne corrige pas automatiquement les ressources non conformes. Lorsque vous désactivez la correction automatique, vous pouvez évaluer les effets de votre nouvelle politique avant de l'appliquer. Lorsque vous êtes convaincu que les modifications sont conformes à vos attentes, modifiez la politique et modifiez l'action de stratégie pour activer la correction automatique.

    Si vous souhaitez plutôt appliquer automatiquement la stratégie aux ressources concernées existantes, choisissez Auto remediate any noncompliant resources (Corriger automatiquement les ressources non conformes). Cette option applique les protections Shield Advanced à chaque compte applicable au sein de l' AWS organisation et à chaque ressource applicable dans les comptes.

    Pour les politiques régionales mondiales uniquement, si vous choisissez Corriger automatiquement les ressources non conformes, vous pouvez également choisir que Firewall Manager remplace automatiquement toutes les associations d'ACL Web AWS WAF classiques existantes par de nouvelles associations aux ACL Web créées à l'aide de la dernière version de AWS WAF (v2). Si vous choisissez cette option, Firewall Manager supprime les associations avec les ACL Web des versions antérieures et crée de nouvelles associations avec les ACL

Web les plus récentes, après avoir créé de nouvelles ACL Web vides dans tous les comptes concernés qui ne les ont pas déjà pour la politique. Pour plus d'informations sur cette option, consultez Remplacez les ACL Web AWS WAF classiques par les ACL Web de dernière version.

11. Choisissez Suivant.
12. Pour Comptes AWS que cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, conservez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.
    - Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

    Vous ne pouvez choisir qu'une des options.

    Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.
13. Choisissez le type de ressource que vous voulez protéger.

    Firewall Manager ne prend pas en charge Amazon Route 53 ou AWS Global Accelerator. Si vous devez utiliser Shield Advanced pour protéger les ressources de ces services, vous ne pouvez pas utiliser une politique de Firewall Manager. Suivez plutôt les instructions de Shield Advanced à l'adresseAjouter AWS Shield Advanced une protection aux AWS ressources.

14. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.
15. Choisissez Suivant.
16. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
17. Choisissez Suivant.
18. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Lorsque vous êtes satisfait de la politique, choisissez Créer une politique. Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

Création d'une stratégie de groupe de sécurité AWS Firewall Manager commune

Pour plus d'informations sur le fonctionnement des stratégies de groupe de sécurité communes, consultez Stratégies de groupe de sécurité communes.

Pour créer une stratégie de groupe de sécurité commune, vous devez avoir déjà créé un groupe de sécurité dans votre compte administrateur Firewall Manager que vous souhaitez utiliser comme principal pour votre stratégie. Vous pouvez gérer les groupes de sécurité via Amazon Virtual Private

Cloud (Amazon VPC) ou Amazon Elastic Compute Cloud (Amazon EC2). Pour plus d'informations, consultez la section Travailler avec des groupes de sécurité dans le guide de l'utilisateur Amazon VPC.

Pour créer une stratégie de groupe de sécurité commune (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour Type de stratégie, choisissez Groupe de sécurité.
5. Pour Security group policy type (Type de stratégie de groupe de sécurité), choisissez Common security groups (Groupes de sécurité communs).
6. Pour Région, choisissez un Région AWS.
7. Choisissez Suivant.
8. Pour Nom de la stratégie, entrez un nom convivial.
9. Pour Règles de stratégie, procédez comme suit :

   a. Dans l'option règles, choisissez les restrictions que vous souhaitez appliquer aux règles du groupe de sécurité et aux ressources relevant du champ d'application de la stratégie. Si vous choisissez Distribuer les balises du groupe de sécurité principal aux groupes de sécurité créés par cette politique, vous devez également sélectionner Identifier et signaler lorsque les groupes de sécurité créés par cette politique deviennent non conformes.

   > **Important**
   >
   > Firewall Manager ne distribuera pas les balises système ajoutées par les AWS services dans les groupes de sécurité répliqués. Les balises système commencent par le préfixe `aws:`. En outre, Firewall Manager ne met pas à jour les balises des

groupes de sécurité existants ni ne crée de nouveaux groupes de sécurité si la politique contient des balises en conflit avec la politique de balises de l'entreprise. Pour plus d'informations sur les politiques relatives aux balises, consultez la section Politiques relatives aux balises dans le guide de AWS Organizations l'utilisateur.

Si vous choisissez Distribuer les références de groupe de sécurité du groupe de sécurité principal aux groupes de sécurité créés par cette politique, Firewall Manager ne distribue les références de groupe de sécurité que s'ils disposent d'une connexion d'appairage active dans Amazon VPC. Pour plus d'informations sur cette option, consultez la section Paramètres des règles de politique.

b. Pour les groupes de sécurité principaux, choisissez Ajouter des groupes de sécurité, puis choisissez les groupes de sécurité que vous souhaitez utiliser. Firewall Manager renseigne la liste des groupes de sécurité de toutes les instances Amazon VPC du compte administrateur de Firewall Manager.

   Par défaut, le nombre maximum de groupes de sécurité principaux par politique est de 3. Pour plus d'informations sur ce paramètre, consultez AWS Firewall Manager quotas.

c. Pour Action de stratégie (Policy action), nous vous recommandons de créer la stratégie avec l'option qui n'applique pas la résolution automatique. Cela vous permet d'évaluer les effets de votre nouvelle stratégie avant d'appliquer celle-ci. Lorsque vous êtes convaincu que les modifications correspondent à vos besoins, modifiez la stratégie et modifiez l'action de stratégie pour activer la résolution automatique des ressources non conformes.

10. Choisissez Suivant.
11. Pour Comptes AWS que cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

- Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

Vous ne pouvez choisir qu'une des options.

Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.

12. Pour Resource type (Type de ressource), choisissez les types de ressources que vous souhaitez protéger.

    Si vous choisissez une instance EC2, vous pouvez choisir d'inclure toutes les interfaces réseau élastiques dans chaque instance Amazon EC2 ou uniquement l'interface par défaut dans chaque instance. Si vous disposez de plusieurs interfaces Elastic Network dans une instance Amazon EC2 incluse, le choix de l'option permettant d'inclure toutes les interfaces permet à Firewall Manager d'appliquer la politique à chacune d'entre elles. Lorsque vous activez la correction automatique, si Firewall Manager ne peut pas appliquer la politique à toutes les interfaces réseau élastiques d'une instance Amazon EC2, il marque l'instance comme non conforme.

13. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ».

Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.

14. Pour les Ressources VPC partagées, si vous souhaitez appliquer la stratégie aux ressources des VPC partagés, outre les VPC que possèdent les comptes, sélectionnez Inclure les ressources des VPC partagés.
15. Choisissez Suivant.
16. Vérifiez les paramètres de stratégie pour vous assurer qu'ils vous conviennent, puis choisissez Créer une stratégie.

Firewall Manager crée une réplique du groupe de sécurité principal dans chaque instance Amazon VPC contenue dans les comptes concernés, dans la limite du quota maximum d'Amazon VPC pris en charge par compte. Firewall Manager associe les répliques de groupes de sécurité aux ressources relevant du champ d'application de la politique pour chaque compte concerné. Pour en savoir plus sur le fonctionnement de cette stratégie, consultez Stratégies de groupe de sécurité communes.

Création d'une stratégie de groupe de sécurité d'audit de contenu AWS Firewall Manager

Pour plus d'informations sur le fonctionnement des stratégies de groupe de sécurité d'audit de contenu, consultez Stratégies de groupe de sécurité d'audit de contenu.

Pour certains paramètres de stratégie d'audit de contenu, vous devez fournir un groupe de sécurité d'audit que Firewall Manager pourra utiliser comme modèle. Par exemple, vous pouvez avoir un groupe de sécurité d'audit qui contient toutes les règles que vous n'autorisez dans aucun des groupes de sécurité. Vous devez créer ces groupes de sécurité d'audit à l'aide de votre compte administrateur Firewall Manager avant de pouvoir les utiliser dans votre politique. Vous pouvez gérer les groupes de sécurité via Amazon Virtual Private Cloud (Amazon VPC) ou Amazon Elastic Compute Cloud (Amazon EC2). Pour plus d'informations, consultez la section Travailler avec des groupes de sécurité dans le guide de l'utilisateur Amazon VPC.

Pour créer une stratégie de groupe de sécurité d'audit de contenu (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

> **Note**
>
> Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour Type de stratégie, choisissez Groupe de sécurité.
5. Pour Security group policy type (Type de stratégie de groupe de sécurité), choisissez Auditing and enforcement of security group rules (Audit et application de règles de groupe de sécurité).
6. Pour Région, choisissez un Région AWS.
7. Choisissez Suivant.
8. Pour Nom de la stratégie, entrez un nom convivial.
9. Pour les règles de stratégie, choisissez l'option de règles de stratégie gérées ou personnalisées que vous souhaitez utiliser.

    a. Pour Configurer les règles de politique d'audit gérées, procédez comme suit :

        i. Pour Configurer les règles de groupe de sécurité à auditer, sélectionnez le type de règles de groupe de sécurité auquel vous souhaitez que votre politique d'audit s'applique.

        ii. Si vous souhaitez notamment appliquer des règles d'audit basées sur les protocoles, les ports et les paramètres de plage d'adresses CIDR de vos groupes de sécurité, choisissez Auditer les règles de groupe de sécurité trop permissives et sélectionnez les options souhaitées.

            Pour la sélection La règle autorise tout le trafic, vous pouvez fournir une liste d'applications personnalisée pour désigner les applications que vous souhaitez auditer. Pour plus d'informations sur les listes d'applications personnalisées et sur leur utilisation dans votre politique, consultez Listes gérées etUtilisation de listes gérées.

            Pour les sélections qui utilisent des listes de protocoles, vous pouvez utiliser des listes existantes et créer de nouvelles listes. Pour plus d'informations sur les listes de protocoles et sur la façon de les utiliser dans votre politique, reportez-vous Listes gérées aux sections etUtilisation de listes gérées.

iii. Si vous souhaitez auditer les applications à haut risque en fonction de leur accès à des plages CIDR réservées ou non réservées, choisissez Auditer les applications à haut risque et sélectionnez les options souhaitées.

Les sélections suivantes s'excluent mutuellement : applications qui peuvent accéder uniquement aux plages d'adresses CIDR réservées et applications autorisées à accéder aux plages d'adresses CIDR non réservées. Vous pouvez sélectionner au plus l'un d'entre eux dans n'importe quelle politique.

Pour les sélections utilisant des listes d'applications, vous pouvez utiliser des listes existantes et créer de nouvelles listes. Pour plus d'informations sur les listes d'applications et sur la façon de les utiliser dans votre politique, consultez Listes gérées etUtilisation de listes gérées.

iv. Utilisez les paramètres de remplacement pour remplacer explicitement les autres paramètres de la politique. Vous pouvez choisir de toujours autoriser ou de toujours refuser des règles de groupe de sécurité spécifiques, qu'elles soient conformes ou non aux autres options que vous avez définies pour la politique.

Pour cette option, vous devez fournir un groupe de sécurité d'audit en tant que modèle de règles autorisées ou de règles refusées. Pour Auditer les groupes de sécurité, choisissez Ajouter des groupes de sécurité d'audit, puis choisissez le groupe de sécurité que vous souhaitez utiliser. Firewall Manager renseigne la liste des groupes de sécurité d'audit à partir de toutes les instances Amazon VPC du compte administrateur de Firewall Manager. Le quota maximal par défaut pour le nombre de groupes de sécurité d'audit pour une stratégie est égal à un (1). Pour de plus amples informations sur l'augmentation du quota, consultez AWS Firewall Manager quotas.

b. Pour Configurer des règles de politique personnalisées, procédez comme suit :

i. Dans les options de règles, choisissez d'autoriser uniquement les règles définies dans les groupes de sécurité d'audit ou de refuser toutes les règles. Pour de plus amples informations sur ce choix, consultez Stratégies de groupe de sécurité d'audit de contenu.

ii. Pour Auditer les groupes de sécurité, choisissez Ajouter des groupes de sécurité d'audit, puis choisissez le groupe de sécurité que vous souhaitez utiliser. Firewall Manager renseigne la liste des groupes de sécurité d'audit à partir de toutes les instances Amazon VPC du compte administrateur de Firewall Manager. Le quota maximal par défaut pour le nombre de groupes de sécurité d'audit pour une stratégie

est égal à un (1). Pour de plus amples informations sur l'augmentation du quota, consultez AWS Firewall Manager quotas.

iii. Pour Action de stratégie (Policy action), vous devez créer la stratégie avec l'option qui n'applique pas la résolution automatique. Cela vous permet d'évaluer les effets de votre nouvelle stratégie avant d'appliquer celle-ci. Lorsque vous êtes convaincu que les modifications correspondent à vos souhaits, modifiez la stratégie et modifiez l'action de stratégie pour activer la résolution automatique des ressources non conformes.

10. Choisissez Suivant.
11. Pour Comptes AWS que cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.
    - Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

    Vous ne pouvez choisir qu'une des options.

    Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.
12. Pour Type de ressource, choisissez les types de ressource que vous souhaitez protéger.

13. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.

14. Choisissez Suivant.
15. Vérifiez les paramètres de stratégie pour vous assurer qu'ils vous conviennent, puis choisissez Créer une stratégie.

Firewall Manager compare le groupe de sécurité d'audit aux groupes de sécurité concernés de votre AWS organisation, conformément aux paramètres de vos règles de politique. Vous pouvez consulter l'état de la politique dans la console des AWS Firewall Manager politiques. Une fois la stratégie créée, vous pouvez la modifier et activer la résolution automatique pour mettre en œuvre votre stratégie de groupe de sécurité d'audit. Pour en savoir plus sur le fonctionnement de cette stratégie, consultez Stratégies de groupe de sécurité d'audit de contenu.

Création d'une stratégie de groupe de sécurité d'audit d'utilisation AWS Firewall Manager

Pour plus d'informations sur le fonctionnement des stratégies de groupe de sécurité d'audit d'utilisation, consultez Stratégies de groupe de sécurité d'audit d'utilisation.

Pour créer une stratégie de groupe de sécurité d'audit d'utilisation (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

> **Note**
>
> Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour Type de stratégie, choisissez Groupe de sécurité.
5. Pour le type de politique de groupe de sécurité, choisissez Audit et nettoyage des groupes de sécurité redondants et non associés.
6. Pour Région, choisissez un Région AWS.
7. Choisissez Suivant.
8. Pour Nom de la stratégie, entrez un nom convivial.
9. Pour Règles de stratégie, choisissez l'une des options disponibles ou les deux.

   - Si vous choisissez que les groupes de sécurité relevant de cette zone de politique doivent être utilisés par au moins une ressource, Firewall Manager supprime tous les groupes de sécurité qu'il juge inutilisés. Lorsque cette règle est activée, Firewall Manager l'exécute en dernier lorsque vous enregistrez la politique.

     Pour plus de détails sur la manière dont Firewall Manager détermine l'utilisation et le calendrier de la correction, consultezStratégies de groupe de sécurité d'audit d'utilisation.

     > **Note**
     >
     > Lorsque vous utilisez ce type de politique de groupe de sécurité d'audit d'utilisation, évitez de modifier plusieurs fois le statut d'association des groupes de sécurité concernés en peu de temps. Cela peut empêcher Firewall Manager de rater les événements correspondants.

     Par défaut, Firewall Manager considère les groupes de sécurité comme non conformes à cette règle de politique dès qu'ils ne sont pas utilisés. Vous pouvez éventuellement spécifier le nombre de minutes pendant lesquelles un groupe de sécurité peut rester inutilisé avant qu'il ne soit considéré comme non conforme, jusqu'à 525 600 minutes (365 jours). Vous pouvez

utiliser ce paramètre pour vous donner le temps d'associer de nouveaux groupes de sécurité à des ressources.

> **Important**
>
> Si vous spécifiez un nombre de minutes autre que la valeur par défaut de zéro, vous devez activer les relations indirectes dans AWS Config. Dans le cas contraire, vos politiques de groupe de sécurité d'audit d'utilisation ne fonctionneront pas comme prévu. Pour plus d'informations sur les relations indirectes dans AWS Config, voir Relations indirectes AWS Config dans le Guide du AWS Config développeur.

- Si vous choisissez que les groupes de sécurité relevant de cette zone de politique doivent être uniques, Firewall Manager consolide les groupes de sécurité redondants, de sorte qu'un seul d'entre eux soit associé aux ressources. Si vous choisissez cette option, Firewall Manager l'exécute d'abord lorsque vous enregistrez la politique.

10. Pour Action de stratégie (Policy action), nous vous recommandons de créer la stratégie avec l'option qui n'applique pas la résolution automatique. Cela vous permet d'évaluer les effets de votre nouvelle stratégie avant d'appliquer celle-ci. Lorsque vous êtes convaincu que les modifications correspondent à vos besoins, modifiez la stratégie et modifiez l'action de stratégie pour activer la résolution automatique des ressources non conformes.
11. Choisissez Suivant.
12. Pour Comptes AWS que cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.
    - Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à

spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

Vous ne pouvez choisir qu'une des options.

Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.

13. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.

14. Choisissez Suivant.
15. Si vous n'avez pas exclu le compte administrateur de Firewall Manager du champ d'application de la politique, Firewall Manager vous invite à le faire. Cela vous permet de contrôler manuellement les groupes de sécurité du compte administrateur de Firewall Manager, que vous utilisez pour les politiques de groupe de sécurité communes et d'audit. Choisissez l'option souhaitée dans cette boîte de dialogue.
16. Vérifiez les paramètres de stratégie pour vous assurer qu'ils vous conviennent, puis choisissez Créer une stratégie.

Si vous avez choisi d'exiger des groupes de sécurité uniques, Firewall Manager recherche des groupes de sécurité redondants dans chaque instance Amazon VPC concernée. Ensuite, si vous choisissez d'exiger que chaque groupe de sécurité soit utilisé par au moins une ressource, Firewall Manager recherche les groupes de sécurité restés inutilisés pendant les minutes spécifiées dans

la règle. Vous pouvez consulter l'état de la politique dans la console des AWS Firewall Manager politiques. Pour en savoir plus sur le fonctionnement de cette stratégie, consultez Stratégies de groupe de sécurité d'audit d'utilisation.

Création d'une politique ACL AWS Firewall Manager réseau

Pour plus d'informations sur le fonctionnement des politiques ACL du réseau, consultezPolitiques ACL du réseau.

Pour créer une politique ACL réseau, vous devez savoir comment définir une ACL réseau à utiliser avec vos sous-réseaux Amazon VPC. Pour plus d'informations, consultez les sections Contrôler le trafic vers les sous-réseaux à l'aide des ACL réseau et Travailler avec des ACL réseau dans le guide de l'utilisateur Amazon VPC.

Pour créer une politique ACL réseau (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour le type de stratégie, choisissez Network ACL.
5. Pour Région, choisissez un Région AWS.
6. Choisissez Suivant.
7. Dans Nom de la politique, entrez un nom descriptif.
8. Pour les règles de politique, définissez les règles que vous souhaitez toujours exécuter dans les ACL réseau que Firewall Manager gère pour vous. Les ACL réseau surveillent et gèrent le trafic entrant et sortant. Ainsi, dans votre politique, vous définissez les règles pour les deux directions.

   Dans les deux sens, vous définissez des règles que vous souhaitez toujours exécuter en premier et des règles que vous souhaitez toujours exécuter en dernier. Dans les listes de contrôle

d'accès réseau gérées par Firewall Manager, les propriétaires de comptes peuvent définir des règles personnalisées à exécuter entre ces première et dernière règles.

9. Pour l'action stratégique, si vous souhaitez identifier les sous-réseaux et les ACL réseau non conformes, mais que vous n'avez pas encore pris de mesures correctives, choisissez Identifier les ressources qui ne sont pas conformes aux règles de politique, mais ne corrigent pas automatiquement. Vous pourrez modifier ces options ultérieurement.

   Si vous souhaitez plutôt appliquer automatiquement la politique aux sous-réseaux concernés existants, choisissez Corriger automatiquement les ressources non conformes. Avec cette option, vous spécifiez également s'il faut forcer la correction lorsque le comportement de gestion du trafic des règles de politique entre en conflit avec les règles personnalisées figurant dans l'ACL du réseau. Que vous forciez ou non la correction, Firewall Manager signale des règles contradictoires dans ses violations de conformité.

10. Choisissez Suivant.

11. Pour Comptes AWS que cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.
    - Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

   Vous ne pouvez choisir qu'une des options.

   Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des

comptes spécifiques, Firewall Manager n'applique pas la politique à de nouveaux comptes différents. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.

12. Pour le type de ressource, le paramètre est fixé aux sous-réseaux.
13. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.
14. Choisissez Suivant.
15. Vérifiez les paramètres de stratégie pour vous assurer qu'ils vous conviennent, puis choisissez Créer une stratégie.

Firewall Manager crée la politique et commence à surveiller et à gérer les ACL du réseau concernés conformément à vos paramètres. Pour en savoir plus sur le fonctionnement de cette stratégie, consultez Politiques ACL du réseau.

Création d'une AWS Firewall Manager politique pour AWS Network Firewall

Dans une politique de Firewall Manager Network Firewall, vous utilisez des groupes de règles que vous gérez AWS Network Firewall. Pour plus d'informations sur la gestion de vos groupes de règles, consultez la section Groupes de AWS Network Firewall règles du Network Firewall Developer Guide.

Pour plus d'informations sur les politiques de Firewall Manager Network Firewall, consultezAWS Network Firewall politiques.

Pour créer une politique Firewall Manager pour AWS Network Firewall (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/

wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

> **Note**
>
> Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour Policy type (Type de stratégie), choisissez AWS Network Firewall.
5. Sous Type de gestion de pare-feu, choisissez la manière dont vous souhaitez que Firewall Manager gère les pare-feux définis par la politique. Sélectionnez parmi les options suivantes :
   - Distribué : Firewall Manager crée et gère des points de terminaison de pare-feu dans chaque VPC concerné par la politique.
   - Centralisé : Firewall Manager crée et gère les points de terminaison dans un seul VPC d'inspection.
   - Importer des pare-feux existants : Firewall Manager importe des pare-feux existants depuis Network Firewall à l'aide d'ensembles de ressources. Pour plus d'informations sur les ensembles de ressources, consultezUtilisation des ensembles de ressources dans Firewall Manager.
6. Pour Région, choisissez un Région AWS. Pour protéger les ressources de plusieurs régions, vous devez créer des politiques distinctes pour chaque région.
7. Choisissez Suivant.
8. Dans Nom de la politique, entrez un nom descriptif. Firewall Manager inclut le nom de la politique dans les noms des pare-feux Network Firewall et des politiques de pare-feu qu'il crée.
9. Dans la configuration AWS Network Firewall de la politique, configurez la politique de pare-feu comme vous le feriez dans Network Firewall. Ajoutez vos groupes de règles apatrides et statiques et spécifiez les actions par défaut de la politique. Vous pouvez éventuellement définir l'ordre d'évaluation dynamique des règles et les actions par défaut de la politique, ainsi que la configuration de journalisation. Pour plus d'informations sur la gestion des politiques de pare-feu de Network Firewall, consultez les politiques de AWS Network Firewall pare-feu dans le Guide du AWS Network Firewall développeur.

Lorsque vous créez la politique Firewall Network Firewall de Firewall Manager, Firewall Manager crée des politiques de pare-feu pour les comptes concernés. Les responsables de comptes individuels peuvent ajouter des groupes de règles aux politiques de pare-feu, mais ils ne peuvent pas modifier la configuration que vous fournissez ici.

10. Choisissez Suivant.
11. Procédez de l'une des manières suivantes, en fonction du type de gestion du pare-feu que vous avez sélectionné à l'étape précédente :

    - Si vous utilisez un type de gestion de pare-feu distribué, dans Configuration du point de AWS Firewall Manager terminaison sous Emplacement du point de terminaison du pare-feu, choisissez l'une des options suivantes :
      - Configuration personnalisée des points de terminaison : Firewall Manager crée des pare-feux pour chaque VPC dans le cadre de la politique, dans les zones de disponibilité que vous spécifiez. Chaque pare-feu contient au moins un point de terminaison.
        - Sous Zones de disponibilité, sélectionnez les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu. Vous pouvez sélectionner des zones de disponibilité par nom de zone de disponibilité ou par ID de zone de disponibilité.
        - Si vous souhaitez fournir les blocs d'adresse CIDR que Firewall Manager utilisera pour les sous-réseaux de pare-feu de vos VPC, ils doivent tous être des blocs d'adresse CIDR /28. Entrez un bloc par ligne. Si vous les omettez, Firewall Manager choisit pour vous les adresses IP parmi celles disponibles dans les VPC.

        > **Note**
        >
        > La correction automatique s'effectue automatiquement pour les politiques de AWS Firewall Manager Network Firewall. Vous ne verrez donc pas d'option vous permettant de ne pas procéder à la correction automatique ici.

      - Configuration automatique des points de terminaison : Firewall Manager crée automatiquement des points de terminaison de pare-feu dans les zones de disponibilité avec des sous-réseaux publics dans votre VPC.
        - Pour la configuration des points de terminaison du pare-feu, spécifiez la manière dont vous souhaitez que les points de terminaison du pare-feu soient gérés par Firewall Manager. Nous vous recommandons d'utiliser plusieurs points de terminaison pour une haute disponibilité.

- Si vous utilisez un type de gestion de pare-feu centralisé, dans Configuration du point de AWS Firewall Manager terminaison sous Configuration du VPC d'inspection, entrez l'ID de AWS compte du propriétaire du VPC d'inspection et l'ID VPC du VPC d'inspection.
  - Sous Zones de disponibilité, sélectionnez les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu. Vous pouvez sélectionner des zones de disponibilité par nom de zone de disponibilité ou par ID de zone de disponibilité.
  - Si vous souhaitez fournir les blocs d'adresse CIDR que Firewall Manager utilisera pour les sous-réseaux de pare-feu de vos VPC, ils doivent tous être des blocs d'adresse CIDR /28. Entrez un bloc par ligne. Si vous les omettez, Firewall Manager choisit pour vous les adresses IP parmi celles disponibles dans les VPC.

    > **Note**
    >
    > La correction automatique s'effectue automatiquement pour les politiques de AWS Firewall Manager Network Firewall. Vous ne verrez donc pas d'option vous permettant de ne pas procéder à la correction automatique ici.

- Si vous utilisez un type de gestion de pare-feu d'importation de pare-feux existants, dans Ensembles de ressources, ajoutez un ou plusieurs ensembles de ressources. Un ensemble de ressources définit les pare-feux Network Firewall existants appartenant au compte de votre entreprise que vous souhaitez gérer de manière centralisée dans le cadre de cette politique. Pour ajouter un ensemble de ressources à la politique, vous devez d'abord créer un ensemble de ressources à l'aide de la console ou de l'PutResourceSetAPI. Pour plus d'informations sur les ensembles de ressources, consultezUtilisation des ensembles de ressources dans Firewall Manager. Pour plus d'informations sur l'importation de pare-feux existants depuis Network Firewall, voir Importer des pare-feux existants.

12. Choisissez Suivant.
13. Si votre politique utilise un type de gestion de pare-feu distribué, sous Gestion des itinéraires, choisissez si Firewall Manager surveillera et alertera sur le trafic qui doit être acheminé via les points de terminaison du pare-feu respectifs.

    > **Note**
    >
    > Si vous choisissez Moniteur, vous ne pourrez pas modifier le paramètre sur Désactivé ultérieurement. La surveillance se poursuit jusqu'à ce que vous supprimiez la politique.

14. Pour le type de trafic, ajoutez éventuellement les points de terminaison du trafic par lesquels vous souhaitez acheminer le trafic pour l'inspection du pare-feu.
15. Pour Autoriser le trafic inter-AZ requis, si vous activez cette option, Firewall Manager considère comme conforme le routage qui envoie le trafic hors d'une zone de disponibilité pour inspection, pour les zones de disponibilité qui ne disposent pas de leur propre point de terminaison de pare-feu. Les zones de disponibilité dotées de points de terminaison doivent toujours inspecter leur propre trafic.
16. Choisissez Suivant.
17. Pour le champ d'application de la politique, dans le cadre de Comptes AWS cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.
    - Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

    Vous ne pouvez choisir qu'une des options.

    Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.
18. Le type de ressource pour les politiques Network Firewall est VPC.

19. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.
20. Choisissez Suivant.
21. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
22. Choisissez Suivant.
23. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Lorsque vous êtes satisfait de la politique, choisissez Créer une politique. Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

Création d'une AWS Firewall Manager politique pour le pare-feu DNS Amazon Route 53 Resolver

Dans une politique de pare-feu DNS Firewall Manager, vous utilisez des groupes de règles que vous gérez dans Amazon Route 53 Resolver DNS Firewall. Pour plus d'informations sur la gestion de vos groupes de règles, consultez la section Gestion des groupes de règles et des règles dans le pare-feu DNS dans le manuel Amazon Route 53 Developer Guide.

Pour plus d'informations sur les politiques de pare-feu DNS de Firewall Manager, consultezPolitiques de pare-feu DNS d'Amazon Route 53 Resolver.

Pour créer une politique Firewall Manager pour Amazon Route 53 Resolver DNS Firewall (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour le type de politique, choisissez le pare-feu Amazon Route 53 Resolver DNS.
5. Pour Région, choisissez un Région AWS. Pour protéger les ressources de plusieurs régions, vous devez créer des politiques distinctes pour chaque région.
6. Choisissez Suivant.
7. Dans Nom de la politique, entrez un nom descriptif.
8. Dans la configuration des politiques, ajoutez les groupes de règles que vous souhaitez que DNS Firewall évalue en premier et en dernier parmi les associations de groupes de règles de vos VPC. Vous pouvez ajouter jusqu'à deux groupes de règles à la politique.

   Lorsque vous créez la politique de pare-feu DNS de Firewall Manager, Firewall Manager crée les associations de groupes de règles, avec les priorités d'association que vous avez fournies, pour les VPC et les comptes concernés. Les responsables de comptes individuels peuvent ajouter des associations de groupes de règles entre votre première et votre dernière association, mais ils ne peuvent pas modifier les associations que vous définissez ici. Pour plus d’informations, consultez Politiques de pare-feu DNS d'Amazon Route 53 Resolver.
9. Choisissez Suivant.
10. Pour Comptes AWS que cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.

- Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.
- Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

Vous ne pouvez choisir qu'une des options.

Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.

11. Le type de ressource pour les politiques de pare-feu DNS est VPC.
12. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.
13. Choisissez Suivant.

14. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
15. Choisissez Suivant.
16. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Lorsque vous êtes satisfait de la politique, choisissez Créer une politique. Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

Création d'une AWS Firewall Manager politique pour Palo Alto Networks Cloud NGFW

Avec une politique Firewall Manager pour Palo Alto Networks Cloud Next Generation Firewall (Palo Alto Networks Cloud NGFW), vous utilisez Firewall Manager pour déployer les ressources NGFW de Palo Alto Networks Cloud et gérer les règles NGFW de manière centralisée sur tous vos comptes. AWS

Pour plus d'informations sur les politiques NGFW du Firewall Manager Palo Alto Networks Cloud, consultez. Politiques NGFW de Palo Alto Networks Cloud Pour plus d'informations sur la configuration et la gestion de Palo Alto Networks Cloud NGFW pour Firewall Manager, consultez le Palo Alto Networks Cloud NGFW de Palo Alto Networks dans la documentation. AWS

Prérequis

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez tous les prérequis avant de passer à l'étape suivante.

Pour créer une politique Firewall Manager pour Palo Alto Networks Cloud NGFW (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/

wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

> **Note**
>
> Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour le type de politique, choisissez Palo Alto Networks Cloud NGFW. Si vous n'êtes pas encore abonné au service Palo Alto Networks Cloud NGFW sur AWS Marketplace, vous devez d'abord le faire. Pour vous abonner à la AWS Marketplace, choisissez View AWS Marketplace details.
5. Pour le modèle de déploiement, choisissez le modèle distribué ou le modèle centralisé. Le modèle de déploiement détermine la manière dont Firewall Manager gère les points de terminaison pour la politique. Avec le modèle distribué, Firewall Manager gère les points de terminaison du pare-feu dans chaque VPC relevant du champ d'application des politiques. Avec le modèle centralisé, Firewall Manager gère un point de terminaison unique dans un VPC d'inspection.
6. Pour Région, choisissez un Région AWS. Pour protéger les ressources de plusieurs régions, vous devez créer des politiques distinctes pour chaque région.
7. Choisissez Suivant.
8. Dans Nom de la politique, entrez un nom descriptif.
9. Dans la configuration de la politique, choisissez la politique de pare-feu Palo Alto Networks Cloud NGFW à associer à cette politique. La liste des politiques de pare-feu Palo Alto Networks Cloud NGFW contient toutes les politiques de pare-feu Palo Alto Networks Cloud NGFW associées à votre client Palo Alto Networks Cloud NGFW. Pour plus d'informations sur la création et la gestion des politiques de pare-feu NGFW de Palo Alto Networks Cloud, consultez la AWS Firewall Manager rubrique Deploy Palo Alto Networks Cloud NGFW pour AWS le guide de déploiement. AWS
10. Pour la journalisation NGFW dans le cloud de Palo Alto Networks, vous pouvez éventuellement choisir le ou les types de journaux NGFW de Palo Alto Networks Cloud à enregistrer conformément à votre politique. Pour plus d'informations sur les types de journaux NGFW de Palo Alto Networks Cloud, voir Configurer la journalisation pour Palo Alto Networks Cloud NGFW on AWS dans le guide de déploiement de Palo Alto Networks Cloud NGFW. AWS

Pour la destination des journaux, spécifiez à quel moment Firewall Manager doit écrire les journaux.

11. Choisissez Suivant.
12. Sous Configurer un point de terminaison de pare-feu tiers, effectuez l'une des opérations suivantes, selon que vous utilisez le modèle de déploiement distribué ou centralisé pour créer vos points de terminaison de pare-feu :

    - Si vous utilisez le modèle de déploiement distribué pour cette politique, sous Zones de disponibilité, sélectionnez les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu. Vous pouvez sélectionner des zones de disponibilité par nom de zone de disponibilité ou par ID de zone de disponibilité.
    - Si vous utilisez le modèle de déploiement centralisé pour cette politique, dans la configuration du point de AWS Firewall Manager terminaison sous Configuration du VPC d'inspection, entrez l'ID de AWS compte du propriétaire du VPC d'inspection et l'ID du VPC d'inspection.
        - Sous Zones de disponibilité, sélectionnez les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu. Vous pouvez sélectionner des zones de disponibilité par nom de zone de disponibilité ou par ID de zone de disponibilité.
13. Si vous souhaitez fournir les blocs d'adresse CIDR que Firewall Manager utilisera pour les sous-réseaux de pare-feu de vos VPC, ils doivent tous être des blocs d'adresse CIDR /28. Entrez un bloc par ligne. Si vous les omettez, Firewall Manager choisit pour vous les adresses IP parmi celles disponibles dans les VPC.

    > **Note**
    >
    > La correction automatique s'effectue automatiquement pour les politiques de AWS Firewall Manager Network Firewall. Vous ne verrez donc pas d'option vous permettant de ne pas procéder à la correction automatique ici.

14. Choisissez Suivant.
15. Pour le champ d'application de la politique, dans le cadre de Comptes AWS cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques,

choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

- Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

Vous ne pouvez choisir qu'une des options.

Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.

16. Le type de ressource pour les politiques Network Firewall est VPC.
17. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.
18. Pour accorder un accès entre comptes, choisissez Télécharger le AWS CloudFormation modèle. Cela télécharge un AWS CloudFormation modèle que vous pouvez utiliser pour créer une AWS CloudFormation pile. Cette pile crée un AWS Identity and Access Management rôle qui accorde

à Firewall Manager des autorisations inter-comptes pour gérer les ressources NGFW Cloud de Palo Alto Networks. Pour plus d'informations sur les piles, reportez-vous à la section Utilisation des piles dans le Guide de l'AWS CloudFormation utilisateur.

19. Choisissez Suivant.
20. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
21. Choisissez Suivant.
22. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Lorsque vous êtes satisfait de la politique, choisissez Créer une politique. Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

Création d'une AWS Firewall Manager politique pour Fortigate Cloud Native Firewall (CNF) en tant que service

Avec une politique Firewall Manager pour Fortigate CNF, vous pouvez utiliser Firewall Manager pour déployer et gérer les ressources Fortigate CNF sur l'ensemble de vos comptes. AWS

Pour plus d'informations sur les politiques CNF de Firewall Manager Fortigate, consultez. Politiques de pare-feu natif du cloud (CNF) de Fortigate en tant que service Pour plus d'informations sur la configuration de Fortigate CNF pour une utilisation avec Firewall Manager, consultez la documentation Fortinet.

Prérequis

Il existe plusieurs étapes obligatoires pour préparer votre compte pour AWS Firewall Manager. Ces étapes sont décrites dans AWS Firewall Manager prérequis. Complétez tous les prérequis avant de passer à l'étape suivante.

Pour créer une politique Firewall Manager pour Fortigate CNF (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez Créer une politique.
4. Pour le type de politique, choisissez Fortigate Cloud Native Firewall (CNF) en tant que service. Si vous n'êtes pas encore abonné au service Fortigate CNF sur le AWS Marketplace, vous devez d'abord le faire. Pour vous abonner à la AWS Marketplace, choisissez View AWS Marketplace details.
5. Pour le modèle de déploiement, choisissez le modèle distribué ou le modèle centralisé.
   Le modèle de déploiement détermine la manière dont Firewall Manager gère les points de terminaison pour la politique. Avec le modèle distribué, Firewall Manager gère les points de terminaison du pare-feu dans chaque VPC relevant du champ d'application des politiques. Avec le modèle centralisé, Firewall Manager gère un point de terminaison unique dans un VPC d'inspection.
6. Pour Région, choisissez un Région AWS. Pour protéger les ressources de plusieurs régions, vous devez créer des politiques distinctes pour chaque région.
7. Choisissez Suivant.
8. Dans Nom de la politique, entrez un nom descriptif.
9. Dans la configuration de la politique, choisissez la politique de pare-feu Fortigate CNF à associer à cette politique. La liste des politiques de pare-feu Fortigate CNF contient toutes les politiques de pare-feu Fortigate CNF associées à votre client Fortigate CNF. Pour plus d'informations sur la création et la gestion de locataires Fortigate CNF, consultez la documentation Fortinet.
10. Choisissez Suivant.

11. Sous Configurer un point de terminaison de pare-feu tiers, effectuez l'une des opérations suivantes, selon que vous utilisez le modèle de déploiement distribué ou centralisé pour créer vos points de terminaison de pare-feu :

    - Si vous utilisez le modèle de déploiement distribué pour cette politique, sous Zones de disponibilité, sélectionnez les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu. Vous pouvez sélectionner des zones de disponibilité par nom de zone de disponibilité ou par ID de zone de disponibilité.
    - Si vous utilisez le modèle de déploiement centralisé pour cette politique, dans la configuration du point de AWS Firewall Manager terminaison sous Configuration du VPC d'inspection, entrez l'ID de AWS compte du propriétaire du VPC d'inspection et l'ID du VPC d'inspection.
        - Sous Zones de disponibilité, sélectionnez les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu. Vous pouvez sélectionner des zones de disponibilité par nom de zone de disponibilité ou par ID de zone de disponibilité.
12. Si vous souhaitez fournir les blocs d'adresse CIDR que Firewall Manager utilisera pour les sous-réseaux de pare-feu de vos VPC, ils doivent tous être des blocs d'adresse CIDR /28. Entrez un bloc par ligne. Si vous les omettez, Firewall Manager choisit pour vous les adresses IP parmi celles disponibles dans les VPC.

    > **Note**
    >
    > La correction automatique s'effectue automatiquement pour les politiques de AWS Firewall Manager Network Firewall. Vous ne verrez donc pas d'option vous permettant de ne pas procéder à la correction automatique ici.

13. Choisissez Suivant.
14. Pour le champ d'application de la politique, dans le cadre de Comptes AWS cette politique s'applique à, choisissez l'option suivante :

    - Si vous souhaitez appliquer la politique à tous les comptes de votre organisation, laissez la sélection par défaut, Inclure tous les comptes de mon AWS organisation.
    - Si vous souhaitez appliquer la politique uniquement à des comptes spécifiques ou à des comptes appartenant à des unités AWS Organizations organisationnelles (UO) spécifiques, choisissez Inclure uniquement les comptes et unités organisationnelles spécifiés, puis ajoutez les comptes et les UO que vous souhaitez inclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités

d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

- Si vous souhaitez appliquer la politique à tous les comptes ou unités d' AWS Organizations organisation (UO) à l'exception d'un ensemble spécifique, choisissez Exclure les comptes et unités organisationnelles spécifiés et incluez tous les autres, puis ajoutez les comptes et les unités d'organisation que vous souhaitez exclure. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.

Vous ne pouvez choisir qu'une des options.

Une fois que vous avez appliqué la politique, Firewall Manager évalue automatiquement les nouveaux comptes par rapport à vos paramètres. Par exemple, si vous n'incluez que des comptes spécifiques, Firewall Manager n'applique cette politique à aucun nouveau compte. Autre exemple, si vous incluez une unité d'organisation, lorsque vous ajoutez un compte à l'unité d'organisation ou à l'une de ses unités d'organisation secondaires, Firewall Manager applique automatiquement la politique au nouveau compte.

15. Le type de ressource pour les politiques Network Firewall est VPC.
16. Pour les ressources, vous pouvez réduire la portée de la politique à l'aide du balisage, en incluant ou en excluant les ressources avec les balises que vous spécifiez. Vous pouvez utiliser l'inclusion ou l'exclusion, mais pas les deux. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.

    Si vous entrez plusieurs balises, une ressource doit avoir toutes les balises à inclure ou à exclure.

    Les balises de ressources ne peuvent avoir que des valeurs non nulles. Si vous omettez la valeur d'une balise, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises qui ont la même clé et la même valeur.
17. Pour accorder un accès entre comptes, choisissez Télécharger le AWS CloudFormation modèle. Cela télécharge un AWS CloudFormation modèle que vous pouvez utiliser pour créer une AWS CloudFormation pile. Cette pile crée un AWS Identity and Access Management rôle qui accorde à Firewall Manager des autorisations entre comptes pour gérer les ressources Fortigate CNF. Pour plus d'informations sur les piles, reportez-vous à la section Utilisation des piles dans le

Guide de l'AWS CloudFormation utilisateur. Pour créer une pile, vous aurez besoin de l'identifiant de compte du portail Fortigate CNF.

18. Choisissez Suivant.
19. Pour les balises de stratégie, ajoutez les balises d'identification que vous souhaitez ajouter à la ressource de politique de Firewall Manager. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
20. Choisissez Suivant.
21. Passez en revue les nouveaux paramètres de politique et revenez à toutes les pages où vous devez apporter des modifications.

    Lorsque vous êtes satisfait de la politique, choisissez Créer une politique. Dans le volet AWS Firewall Manager des politiques, votre politique doit être répertoriée. Il indiquera probablement En attente sous les en-têtes des comptes et indiquera l'état du paramètre de correction automatique. La création d'une stratégie peut prendre plusieurs minutes. Une fois que le statut Pending (En attente) est remplacé par le nombre de comptes, vous pouvez choisir le nom de la stratégie pour examiner le statut de conformité des comptes et des ressources. Pour plus d'informations, veuillez consulter Afficher les informations de conformité d'une AWS Firewall Manager politique

Supprimer une AWS Firewall Manager politique

Vous pouvez supprimer une stratégie Firewall Manager en effectuant les étapes suivantes.

Pour supprimer une stratégie (console)

1. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
2. Choisissez l'option en regard de la stratégie que vous voulez supprimer.
3. Sélectionnez Delete (Supprimer).

> **Note**
>
> Lorsque vous supprimez une stratégie de groupe de sécurité commune de Firewall Manager, pour supprimer les groupes de sécurité répliqués de la politique, choisissez l'option permettant de nettoyer les ressources créées par la politique. Dans le cas contraire, une

fois le serveur principal supprimé, les répliques sont conservées et nécessitent une gestion manuelle dans chaque instance Amazon VPC.

Important

Lorsque vous supprimez une politique Firewall Manager Shield Advanced, celle-ci est supprimée, mais vos comptes restent abonnés à Shield Advanced.

AWS Firewall Manager portée de la politique

Le champ d'application de la politique définit les domaines dans lesquels la politique s'applique. Vous pouvez appliquer des politiques contrôlées de manière centralisée à tous vos comptes et ressources au sein de votre organisation ou à un sous-ensemble de vos comptes et ressources. AWS Organizations Pour obtenir des instructions sur la façon de définir le champ d'application de la politique, consultezCréation d'une AWS Firewall Manager politique.

Options du champ d'application de la politique dans AWS Firewall Manager

Lorsque vous ajoutez un nouveau compte ou une nouvelle ressource à votre organisation, Firewall Manager l'évalue automatiquement par rapport à vos paramètres pour chaque politique et applique la politique en fonction de ces paramètres. Par exemple, vous pouvez choisir d'appliquer une politique à tous les comptes à l'exception des numéros de compte figurant dans une liste spécifiée ; vous pouvez également choisir d'appliquer une politique uniquement aux ressources qui possèdent toutes les balises d'une liste.

Comptes AWS dans le champ d'application

Les paramètres que vous définissez pour définir les comptes Comptes AWS concernés par la politique déterminent les comptes de votre AWS organisation auxquels appliquer la politique. Vous pouvez choisir d'appliquer la stratégie de l'une des manières suivantes :

- À tous les comptes de votre organisation
- À seulement une liste spécifique de numéros de compte et d'unités d’organisation AWS Organizations inclus
- À tous les éléments sauf une liste spécifique de numéros de compte et d'unités d’organisation AWS Organizations exclus

Pour plus d'informations AWS Organizations, consultez le Guide de AWS Organizations l'utilisateur.

Ressources concernées

Comme pour les comptes concernés, les paramètres que vous fournissez pour les ressources déterminent les types de ressources concernés auxquels appliquer la politique. Vous pouvez choisir l'une des méthodes suivantes.

- Toutes les ressources
- Ressources contenant toutes les balises que vous spécifiez
- Toutes les ressources sauf celles qui ont toutes les balises que vous spécifiez

Vous ne pouvez spécifier des balises de ressources qu'avec des valeurs non nulles. Si vous ne fournissez rien pour la valeur, Firewall Manager enregistre la balise avec une valeur de chaîne vide : « ». Les balises de ressources correspondent uniquement aux balises ayant la même clé et la même valeur.

Pour plus d'informations sur le balisage de vos ressources, consultez Utilisation de l'éditeur de balises.

Gestion du périmètre des politiques dans AWS Firewall Manager

Lorsque des politiques sont en place, Firewall Manager les gère en permanence et les applique aux nouvelles ressources au fur Comptes AWS et à mesure qu'elles sont ajoutées, conformément au champ d'application de la politique.

Comment Firewall Manager gère ses ressources Comptes AWS et gère ses ressources

Si un compte ou une ressource sort du champ d'application pour une raison quelconque, AWS Firewall Manager cela ne supprime pas automatiquement les protections ou ne supprime pas les ressources gérées par Firewall Manager, sauf si vous cochez la case Supprimer automatiquement les protections des ressources qui quittent le champ d'application de la politique.

> **Note**
>
> L'option Supprimer automatiquement les protections des ressources qui quittent le champ d'application de la politique n'est pas disponible pour AWS Shield Advanced les politiques AWS WAF classiques.

Cette case à cocher permet de AWS Firewall Manager nettoyer automatiquement les ressources gérées par Firewall Manager pour les comptes lorsque ces comptes quittent le champ d'application de la politique. Par exemple, Firewall Manager dissocie une ACL Web gérée par Firewall Manager d'une ressource client protégée lorsque la ressource client quitte le champ d'application de la politique.

Pour déterminer quelles ressources doivent être retirées de la protection lorsqu'une ressource client quitte le champ d'application de la politique, Firewall Manager suit les directives suivantes :

- Comportement par défaut :
  - Les règles AWS Config gérées associées sont supprimées. Ce comportement est indépendant de la case à cocher.
  - Toutes les listes de contrôle d'accès AWS WAF Web (ACL Web) associées ne contenant aucune ressource sont supprimées. Ce comportement est indépendant de la case à cocher.
  - Toute ressource protégée qui sort de son champ d'application reste associée et protégée. Par exemple, une Application Load Balancer ou une API d'API Gateway associée à une ACL Web reste associée à l'ACL Web et la protection reste en place.
- Lorsque la case Supprimer automatiquement les protections des ressources qui quittent le champ d'application de la politique est cochée :
  - Les règles AWS Config gérées associées sont supprimées. Ce comportement est indépendant de la case à cocher.
  - Toutes les listes de contrôle d'accès AWS WAF Web (ACL Web) associées ne contenant aucune ressource sont supprimées. Ce comportement est indépendant de la case à cocher.
  - Toute ressource protégée qui sort du champ d'application est automatiquement dissociée et supprimée de la protection de Firewall Manager lorsqu'elle quitte le champ d'application de la politique. Par exemple, pour une politique de groupe de sécurité, une instance d'accélérateur Elastic Inference ou d'Amazon EC2 est automatiquement dissociée du groupe de sécurité répliqué lorsqu'elle quitte le champ d'application de la politique. Le groupe de sécurité répliqué et ses ressources sont automatiquement retirés de la protection.

Listes gérées

Les listes d'applications et de protocoles gérées rationalisent la configuration et la gestion des politiques de groupe de sécurité relatives à l'audit de AWS Firewall Manager contenu. Vous utilisez des listes gérées pour définir les protocoles et les applications autorisés et interdits par votre

politique. Pour plus d'informations sur les politiques de groupe de sécurité relatives à l'audit de contenu, consultezStratégies de groupe de sécurité d'audit de contenu.

Vous pouvez utiliser les types de listes gérées suivants dans une stratégie de groupe de sécurité d'audit de contenu :

- Listes d'applications et listes de protocoles Firewall Manager : Firewall Manager gère ces listes.
  - Les listes d'applications incluent `FMS-Default-Public-Access-Apps-Allowed` et`FMS-Default-Public-Access-Apps-Denied`, qui décrivent les applications couramment utilisées qui devraient être autorisées ou refusées au grand public.
  - Les listes de protocoles incluent `FMS-Default-Protocols-Allowed` une liste de protocoles couramment utilisés qui devraient être autorisés au grand public. Vous pouvez utiliser n'importe quelle liste gérée par Firewall Manager, mais vous ne pouvez ni la modifier ni la supprimer.
- Listes d'applications et listes de protocoles personnalisées : vous gérez ces listes. Vous pouvez créer des listes de l'un ou l'autre type avec les paramètres dont vous avez besoin. Vous avez le contrôle total de vos propres listes gérées personnalisées, et vous pouvez les créer, les modifier et les supprimer selon vos besoins.

> **Note**
>
> À l'heure actuelle, Firewall Manager ne vérifie pas les références à une liste gérée personnalisée lorsque vous la supprimez. Cela signifie que vous pouvez supprimer une liste d'applications ou de protocoles gérée personnalisée même lorsqu'elle est utilisée par une politique active. Cela peut entraîner l'arrêt du fonctionnement de la politique. Supprimez une liste d'applications ou une liste de protocoles uniquement après avoir vérifié qu'elle n'est référencée par aucune politique active.

Les listes gérées sont AWS des ressources. Vous pouvez baliser une liste gérée personnalisée. Vous ne pouvez pas baliser une liste gérée par Firewall Manager.

Gestion des versions des listes

Les listes gérées personnalisées n'ont pas de versions. Lorsque vous modifiez une liste personnalisée, les politiques qui y font référence utilisent automatiquement la liste mise à jour.

Les listes gérées par Firewall Manager sont versionnées. L'équipe du service Firewall Manager publie les nouvelles versions selon les besoins, afin d'appliquer les meilleures pratiques de sécurité aux listes.

Lorsque vous utilisez une liste gérée par Firewall Manager dans une politique, vous choisissez votre stratégie de gestion des versions comme suit :

- Dernière version disponible : si vous ne spécifiez pas de paramètre de version explicite pour la liste, votre politique utilise automatiquement la dernière version. Il s'agit de la seule option disponible via la console.
- Version explicite : si vous spécifiez une version pour la liste, votre politique utilise cette version. Votre politique reste verrouillée sur la version que vous avez spécifiée jusqu'à ce que vous modifiiez le paramètre de version. Pour spécifier la version, vous devez définir la politique en dehors de la console, par exemple via la CLI ou l'un des SDK.

Pour plus d'informations sur le choix du paramètre de version pour une liste, consultezUtilisation de listes gérées dans vos politiques de groupe de sécurité d'audit de contenu.

Utilisation de listes gérées dans vos politiques de groupe de sécurité d'audit de contenu

Lorsque vous créez une stratégie de groupe de sécurité d'audit de contenu, vous pouvez choisir d'utiliser des règles de stratégie d'audit gérées. Certains paramètres de cette option nécessitent une liste d'applications gérées ou une liste de protocoles. Ces paramètres incluent, par exemple, les protocoles autorisés dans les règles des groupes de sécurité et les applications pouvant accéder à Internet.

Les restrictions suivantes s'appliquent à chaque paramètre de stratégie qui utilise une liste gérée :

- Vous pouvez spécifier au plus une liste gérée par Firewall Manager pour chaque paramètre. Par défaut, vous pouvez spécifier au plus une liste personnalisée. La limite de liste personnalisée est un quota souple, vous pouvez donc en demander l'augmentation. Pour plus d’informations, consultez AWS Firewall Manager quotas.
- Dans la console, si vous sélectionnez une liste gérée par Firewall Manager, vous ne pouvez pas spécifier la version. La politique utilisera toujours la dernière version de la liste. Pour spécifier la version, vous devez définir la politique en dehors de la console, par exemple via la CLI ou l'un des SDK. Pour plus d'informations sur le versionnement des listes gérées par Firewall Manager, consultezGestion des versions des listes.

Pour plus d'informations sur la création d'une politique de groupe de sécurité d'audit de contenu via la console, consultezCréation d'une stratégie de groupe de sécurité d'audit de contenu.

Création d'une liste d'applications gérées personnalisée

Pour créer une liste d'applications gérées personnalisée

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Listes d'applications.
3. Sur la page des listes d'applications, choisissez Créer une liste d'applications.
4. Sur la page Créer une liste d'applications, donnez un nom à votre liste. N'utilisez pas le préfixe `fms-` car il est réservé à Firewall Manager.
5. Spécifiez une application soit en fournissant le protocole et le numéro de port, soit en sélectionnant une application dans le menu déroulant Type. Donnez un nom aux spécifications de votre application.
6. Choisissez Ajouter un autre formulaire si nécessaire et renseignez les informations de candidature jusqu'à ce que vous ayez complété votre liste.
7. (Facultatif) Appliquez des balises à votre liste.
8. Choisissez Enregistrer pour enregistrer votre liste et revenir à la page des listes d'applications.

Création d'une liste de protocoles gérés personnalisée

Pour créer une liste de protocoles gérés personnalisée

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

> **Note**
>
> Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Protocol lists.
3. Dans la page Listes de protocoles, choisissez Créer une liste de protocoles.
4. Sur la page de création de la liste de protocoles, nommez votre liste. N'utilisez pas le préfixe `fms-` car il est réservé à Firewall Manager.
5. Spécifiez un protocole.
6. Choisissez Ajouter un autre protocole si nécessaire et renseignez les informations du protocole jusqu'à ce que vous ayez terminé votre liste.
7. (Facultatif) Appliquez des balises à votre liste.
8. Choisissez Enregistrer pour enregistrer votre liste et revenir à la page des listes de protocoles.

Afficher une liste gérée

Pour consulter une liste d'applications ou une liste de protocoles

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Listes d'applications ou Listes de protocoles.

   La page affiche toutes les listes du type sélectionné que vous pouvez utiliser. Les listes gérées par Firewall Manager ont un Y dans la ManagedListcolonne.
3. Pour voir les détails d'une liste, choisissez son nom. La page détaillée affiche le contenu de la liste et les éventuelles balises.

Pour les listes gérées par Firewall Manager, vous pouvez également voir les versions disponibles en sélectionnant le menu déroulant Version.

Supprimer une liste gérée personnalisée

Vous pouvez supprimer des listes gérées personnalisées. Vous ne pouvez ni modifier ni supprimer les listes gérées par Firewall Manager.

> **Note**
>
> À l'heure actuelle, Firewall Manager ne vérifie pas les références à une liste gérée personnalisée lorsque vous la supprimez. Cela signifie que vous pouvez supprimer une liste d'applications ou de protocoles gérée personnalisée même lorsqu'elle est utilisée par une politique active. Cela peut entraîner l'arrêt du fonctionnement de la politique. Ne supprimez une liste d'applications ou une liste de protocoles qu'après avoir vérifié qu'elle n'est référencée par aucune politique active.

Pour supprimer une liste d'applications ou de protocoles gérés personnalisés

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Assurez-vous que la liste que vous souhaitez supprimer n'est utilisée dans aucune de vos politiques de groupe de sécurité d'audit en procédant comme suit :

   a. Dans le volet de navigation, sélectionnez Stratégies de sécurité.

   b. Sur la page des AWS Firewall Manager politiques, sélectionnez et modifiez vos groupes de sécurité d'audit, puis supprimez toutes les références à la liste personnalisée que vous souhaitez supprimer.

Si vous supprimez une liste gérée personnalisée utilisée dans une stratégie de groupe de sécurité d'audit, la stratégie qui l'utilise peut cesser de fonctionner.

3. Dans le volet de navigation, choisissez Listes d'applications ou Listes de protocoles, selon le type de liste que vous souhaitez supprimer.
4. Sur la page de liste, sélectionnez la liste personnalisée que vous souhaitez supprimer et choisissez Supprimer.

AWS WAF politiques

Dans une AWS WAF politique Firewall Manager, vous spécifiez les groupes de AWS WAF règles que vous souhaitez utiliser dans l'ensemble de vos ressources. Lorsque vous appliquez la politique, Firewall Manager crée des ACL Web dans les comptes relevant du champ d'application de la politique en fonction de la façon dont vous configurez la gestion des ACL Web dans votre stratégie. Dans les ACL Web créées par la politique, les responsables de comptes individuels peuvent ajouter des règles et des groupes de règles, en plus des groupes de règles que vous avez définis via Firewall Manager.

Comment Firewall Manager gère les ACL Web

Firewall Manager crée des ACL Web en fonction de la façon dont vous configurez le paramètre Gérer les ACL Web non associées dans votre politique ou du `optimizeUnassociatedWebACL` paramètre du type de SecurityServicePolicyDatadonnées dans l'API.

Si vous activez la gestion des ACL Web non associées, Firewall Manager crée des ACL Web dans les comptes relevant du champ d'application de la politique uniquement si les ACL Web doivent être utilisées par au moins une ressource. À tout moment, si un compte entre dans le champ d'application de la politique, Firewall Manager crée automatiquement une ACL Web dans le compte si au moins une ressource utilise l'ACL Web. Lorsque vous activez la gestion des ACL Web non associées, Firewall Manager effectue un nettoyage unique des ACL Web non associées dans votre compte. Pendant le nettoyage, Firewall Manager ignore toutes les ACL Web que vous avez modifiées après leur création, par exemple si vous avez ajouté un groupe de règles à l'ACL Web ou modifié ses paramètres. Le processus de nettoyage peut prendre plusieurs heures. Si une ressource quitte le champ d'application de la politique après que Firewall Manager a créé une ACL Web, Firewall Manager dissocie la ressource de l'ACL Web, mais ne nettoie pas l'ACL Web non associée. Firewall Manager nettoie les ACL Web non associées uniquement lorsque vous activez pour la première fois la gestion des ACL Web non associées dans une politique.

Si vous n'activez pas cette option, Firewall Manager ne gère pas les ACL Web non associées et Firewall Manager crée automatiquement une ACL Web dans chaque compte relevant du champ d'application de la politique.

Échantillonnage et CloudWatch mesures

AWS Firewall Manager active l'échantillonnage et CloudWatch les métriques Amazon pour les ACL Web et les groupes de règles qu'il crée pour une AWS WAF politique.

Structure de dénomination Web ACL

Lorsque Firewall Manager crée une ACL Web pour la politique, il la nomme ACL WebFMManagedWebACLV2-*policy name*-*timestamp*. L'horodatage est exprimé en millisecondes UTC. Par exemple, `FMManagedWebACLV2-MyWAFPolicyName-1621880374078`.

> **Note**
>
> Si une ressource configurée avec une atténuation automatique avancée des attaques DDoS au niveau de la couche application entre dans le champ d'application d'une AWS WAF stratégie, Firewall Manager ne pourra pas associer l'ACL Web créée par la AWS WAF politique à la ressource.

Groupes de règles dans AWS WAF les politiques

Les ACL Web qui sont gérées par les AWS WAF politiques de Firewall Manager contiennent trois ensembles de règles. Ces ensembles fournissent un niveau supérieur de hiérarchisation des règles et des groupes de règles dans la liste ACL web :

- Premiers groupes de règles, définis par vos soins dans la AWS WAF politique de Firewall Manager. AWS WAF évalue d'abord ces groupes de règles.
- Règles et groupes de règles définis par les gestionnaires de comptes dans les listes ACL web. AWS WAF évalue ensuite les règles ou groupes de règles gérés par un compte.
- Derniers groupes de règles, définis par vos soins dans la AWS WAF politique de Firewall Manager. AWS WAF évalue ces groupes de règles en dernier.

Dans chacun de ces ensembles de règles, AWS WAF évalue les règles et les groupes de règles comme d'habitude, en fonction de leurs paramètres de priorité au sein de l'ensemble.

Dans les premier et dernier ensembles de groupes de règles de la stratégie, vous ne pouvez ajouter que des groupes de règles. Vous pouvez utiliser des groupes de règles gérés, que les règles AWS gérées et AWS Marketplace les vendeurs créent et gèrent pour vous. Vous pouvez également gérer et utiliser vos propres groupes de règles. Pour de plus amples informations sur l'ensemble de ces options, veuillez consulter AWS WAF groupes de règles.

Si vous souhaitez utiliser vos propres groupes de règles, vous devez les créer avant de créer votre AWS WAF politique Firewall Manager. Pour de plus amples informations, consultez Gestion de vos propres groupes de règles. Pour utiliser une règle personnalisée individuelle, vous devez définir votre propre groupe de règles, définir votre règle à l'intérieur de celui-ci, puis utiliser le groupe de règles dans votre stratégie.

Les premier et dernier groupes de AWS WAF règles que vous gérez via Firewall Manager ont des noms qui commencent respectivement par `PREFMManaged-` ou `POSTFMManaged-` sont suivis du nom de la politique de Firewall Manager et de l'horodatage de création du groupe de règles, en millisecondes UTC. Par exemple, `PREFMManaged-MyWAFPolicyName-1621880555123`.

Pour plus d'informations sur le mode AWS WAF d'évaluation des requêtes Web, consultezÉvaluation des règles ACL Web et des groupes de règles.

Pour la procédure de création d'une AWS WAF politique Firewall Manager, consultezCréation d'une AWS Firewall Manager politique pour AWS WAF.

Firewall Manager active l'échantillonnage et CloudWatch les métriques Amazon pour les groupes de règles que vous définissez pour la AWS WAF politique.

Les propriétaires de comptes individuels ont un contrôle total sur les mesures et la configuration d'échantillonnage pour toute règle ou groupe de règles qu'ils ajoutent aux ACL Web gérées par la politique.

Configuration de la journalisation pour une AWS WAF politique

Vous pouvez activer la journalisation centralisée pour vos AWS WAF politiques afin d'obtenir des informations détaillées sur le trafic analysé par votre ACL Web au sein de votre organisation. Les informations contenues dans les journaux incluent l'heure à laquelle la demande AWS WAF a été reçue de la part de votre AWS ressource, des informations détaillées sur la demande et l'action correspondant à la règle selon laquelle chaque demande correspond à partir de tous les comptes concernés. Vous pouvez envoyer vos journaux vers un flux de données Amazon Data Firehose ou un bucket Amazon Simple Storage Service (S3). Pour plus d'informations sur la AWS

WAF journalisation, consultez Journalisation AWS WAF du trafic ACL Web le guide du AWS WAF développeur.

> **Note**
>
> AWS Firewall Manager prend en charge cette option pour AWS WAFV2, pas pour AWS WAF Classic.

Rubriques

- Destinations de journalisation
- Activation de la journalisation
- Désactivation de la journalisation

Destinations de journalisation

Cette section décrit les destinations de journalisation que vous pouvez choisir pour envoyer vos journaux AWS WAF de politiques. Chaque section fournit des conseils pour la configuration de la journalisation pour le type de destination et des informations sur tout comportement spécifique au type de destination. Après avoir configuré votre destination de journalisation, vous pouvez fournir ses spécifications à votre AWS WAF politique Firewall Manager pour commencer à vous y connecter.

Firewall Manager n'a aucune visibilité sur les échecs de journalisation une fois la configuration de journalisation créée. Il est de votre responsabilité de vérifier que la livraison du journal fonctionne comme prévu.

> **Note**
>
> Firewall Manager ne modifie aucune configuration de journalisation existante dans les comptes membres de votre organisation.

Rubriques

- Flux de données Amazon Data Firehose
- Compartiments Amazon Simple Storage Service

Flux de données Amazon Data Firehose

Cette rubrique fournit des informations sur l'envoi de vos journaux de trafic ACL Web vers un flux de données Amazon Data Firehose.

Lorsque vous activez la journalisation d'Amazon Data Firehose, Firewall Manager envoie les journaux depuis les ACL Web de votre politique vers un Amazon Data Firehose où vous avez configuré une destination de stockage. Une fois la journalisation activée, AWS WAF envoie les journaux pour chaque ACL Web configurée, via le point de terminaison HTTPS de Kinesis Data Firehose, à la destination de stockage configurée. Avant de l'utiliser, testez votre flux de diffusion pour vous assurer qu'il dispose d'un débit suffisant pour accueillir les journaux de votre organisation. Pour plus d'informations sur la façon de créer un Amazon Kinesis Data Firehose et de consulter les journaux enregistrés, consultez What Is Amazon Data Firehose ?

Vous devez disposer des autorisations suivantes pour activer correctement la journalisation avec un Kinesis :

- `iam:CreateServiceLinkedRole`
- `firehose:ListDeliveryStreams`
- `wafv2:PutLoggingConfiguration`

Lorsque vous configurez une destination de journalisation Amazon Data Firehose sur une AWS WAF politique, Firewall Manager crée une ACL Web pour la politique dans le compte administrateur de Firewall Manager comme suit :

- Firewall Manager crée l'ACL Web dans le compte administrateur de Firewall Manager, que le compte soit ou non concerné par la politique.
- La journalisation est activée sur l'ACL Web, avec un nom de journal`FMManagedWebACLV2-Logging`*`policy name`*`-`*`timestamp`*, l'horodatage étant l'heure UTC à laquelle le journal a été activé pour l'ACL Web, en millisecondes. Par exemple, `FMManagedWebACLV2-LoggingMyWAFPolicyName-1621880565180`. L'ACL Web ne possède aucun groupe de règles ni aucune ressource associée.
- L'ACL Web vous est facturée conformément aux directives AWS WAF tarifaires. Pour plus d'informations, consultez Tarification d'AWS WAF.
- Firewall Manager supprime l'ACL Web lorsque vous supprimez la politique.

Pour plus d'informations sur les rôles liés aux services et les `iam:CreateServiceLinkedRole` autorisations, consultez. Utilisation de rôles liés à un service pour AWS WAF

Pour plus d'informations sur la création de votre flux de diffusion, consultez Création d'un flux de diffusion Amazon Data Firehose.

Compartiments Amazon Simple Storage Service

Cette rubrique fournit des informations sur l'envoi de vos journaux de trafic ACL Web vers un compartiment Amazon S3.

Le bucket que vous choisissez comme destination de journalisation doit appartenir à un compte administrateur de Firewall Manager. Pour plus d'informations sur les exigences relatives à la création de votre compartiment Amazon S3 pour la journalisation et les exigences en matière de dénomination des compartiments, consultez Amazon Simple Storage Service dans le guide du AWS WAF développeur.

Cohérence à terme

Lorsque vous modifiez AWS WAF les politiques configurées avec une destination de journalisation Amazon S3, Firewall Manager met à jour la politique de compartiment pour ajouter les autorisations nécessaires à la journalisation. Ce faisant, Firewall Manager suit les modèles de last-writer-wins sémantique et de cohérence des données utilisés par Amazon Simple Storage Service. Si vous effectuez plusieurs mises à jour de politique simultanément sur une destination Amazon S3 dans la console Firewall Manager ou via l'PutPolicyAPI, certaines autorisations risquent de ne pas être enregistrées. Pour plus d'informations sur le modèle de cohérence des données Amazon S3, consultez le modèle de cohérence des données Amazon S3 dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Autorisations pour publier des journaux dans un compartiment Amazon S3

La configuration de la journalisation du trafic ACL Web pour un compartiment Amazon S3 dans une AWS WAF politique nécessite les paramètres d'autorisation suivants. Firewall Manager attache automatiquement ces autorisations à votre compartiment Amazon S3 lorsque vous configurez Amazon S3 comme destination de journalisation afin d'autoriser le service à publier des journaux dans le compartiment. Si vous souhaitez gérer un accès plus précis à vos ressources de journalisation et de Firewall Manager, vous pouvez définir ces autorisations vous-même. Pour plus d'informations sur la gestion des autorisations, consultez la section Gestion de l'accès aux AWS ressources dans le Guide de l'utilisateur IAM. Pour plus d'informations sur les politiques AWS WAF gérées, consultezAWS politiques gérées pour AWS WAF.

```
{
    "Version": "2012-10-17",
    "Id": "AWSLogDeliveryForFirewallManager",
    "Statement": [
        {
            "Sid": "AWSLogDeliveryAclCheckFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:GetBucketAcl",
            "Resource": "arn:aws:s3:::aws-waf-DOC-EXAMPLE-BUCKET"
        },
        {
            "Sid": "AWSLogDeliveryWriteFMS",
            "Effect": "Allow",
            "Principal": {
                "Service": "delivery.logs.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/
AWSLogs/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Pour éviter le problème de confusion entre les services adjoints, vous pouvez ajouter les clés de contexte `aws:SourceArn`et de condition `aws:SourceAccount`globale à la politique de votre compartiment. Pour ajouter ces clés, vous pouvez soit modifier la politique créée par Firewall Manager lorsque vous configurez la destination de journalisation, soit créer votre propre stratégie si vous souhaitez un contrôle plus précis. Si vous ajoutez ces conditions à votre politique de destination de journalisation, Firewall Manager ne validera ni ne surveillera les protections secondaires confuses. Pour des informations générales sur le problème des députés confus, voir Le problème des députés confus dans le guide de l'utilisateur IAM.

Lorsque vous `sourceAccount` ajoutez les `sourceArn` propriétés d'ajout, cela augmente la taille de la politique du compartiment. Si vous `sourceAccount` ajoutez une longue liste de `sourceArn` propriétés d'ajout, veillez à ne pas dépasser le quota de taille des compartiments fixé par la politique Amazon S3.

L'exemple suivant montre comment éviter le problème de confusion des adjoints en utilisant les clés de contexte `aws:SourceArn` et de condition `aws:SourceAccount` globale dans la politique de votre compartiment. Remplacez *`member-account-id`*par les identifiants de compte des membres de votre 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-DOC-EXAMPLE-BUCKET",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":[
                  "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id:*",
                  "arn:aws:logs:*:member-account-id:*"
               ]
            }
         }
      },
      {
         "Sid":"AWSLogDeliveryWriteFMS",
         "Effect":"Allow",
         "Principal":{
            "Service":"delivery.logs.amazonaws.com"
```

```
         },
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::aws-waf-logs-DOC-EXAMPLE-BUCKET/policy-id/AWSLogs/*",
         "Condition":{
            "StringEquals":{
               "s3:x-amz-acl":"bucket-owner-full-control",
               "aws:SourceAccount":[
                    "member-account-id",
                  "member-account-id"
               ]
            },
            "ArnLike":{
               "aws:SourceArn":[
                  "arn:aws:logs:*:member-account-id-1:*",
                  "arn:aws:logs:*:member-account-id-2:*"
               ]
            }
         }
      }
   ]
}
```

Chiffrement côté serveur pour les compartiments Amazon S3

Vous pouvez activer le chiffrement côté serveur Amazon S3 ou utiliser une clé gérée par AWS Key Management Service le client sur votre compartiment S3. Si vous choisissez d'utiliser le chiffrement Amazon S3 par défaut sur votre compartiment Amazon S3 pour AWS WAF les journaux, vous n'avez aucune action particulière à effectuer. Toutefois, si vous choisissez d'utiliser une clé de chiffrement fournie par le client pour chiffrer vos données Amazon S3 au repos, vous devez ajouter la déclaration d'autorisation suivante à votre AWS Key Management Service politique en matière de clés :

```
{
            "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": "*"
}
```

Pour plus d'informations sur l'utilisation des clés de chiffrement fournies par le client avec Amazon S3, consultez la section Utilisation du chiffrement côté serveur avec des clés fournies par le client (SSE-C) dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Activation de la journalisation

La procédure suivante décrit comment activer la journalisation d'une AWS WAF politique dans la console Firewall Manager.

Pour activer la journalisation pour une AWS WAF politique

1. Avant de pouvoir activer la journalisation, vous devez configurer vos ressources de destination de journalisation comme suit :

   - Amazon Kinesis Data Streams : créez un Amazon Data Firehose à l'aide de votre compte administrateur Firewall Manager. Utilisez un nom commençant par le préfixe`aws-waf-logs-`. Par exemple, `aws-waf-logs-firewall-manager-central`. Créez le pare-feu de données avec une PUT source et dans la région dans laquelle vous opérez. Si vous capturez des journaux pour Amazon CloudFront, créez le firehose dans l'est des États-Unis (Virginie du Nord). Avant de l'utiliser, testez votre flux de diffusion pour vous assurer qu'il dispose d'un débit suffisant pour accueillir les journaux de votre organisation. Pour plus d'informations, consultez Création d'un flux de diffusion Amazon Data Firehose.
   - Compartiments Amazon Simple Storage Service : créez un compartiment Amazon S3 conformément aux instructions de la rubrique Amazon Simple Storage Service du guide du AWS WAF développeur. Vous devez également configurer votre compartiment Amazon S3 avec les autorisations répertoriées dansAutorisations pour publier des journaux dans un compartiment Amazon S3 .
2. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

> **Note**
>
> Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

3. Dans le volet de navigation, sélectionnez Security Policies.
4. Choisissez la AWS WAF politique pour laquelle vous souhaitez activer la journalisation. Pour plus d'informations sur la journalisation AWS WAF , consultez Journalisation AWS WAF du trafic ACL Web.
5. Dans l'onglet Détails de la politique, dans la section Règles de politique, choisissez Modifier.
6. Pour la configuration de la journalisation, choisissez Activer la journalisation pour activer la journalisation. La journalisation fournit des informations détaillées sur le trafic analysé par votre ACL Web. Choisissez la destination de journalisation, puis choisissez la destination de journalisation que vous avez configurée. Vous devez choisir une destination de journalisation dont le nom commence par`aws-waf-logs-`. Pour plus d'informations sur la configuration d'une destination de AWS WAF journalisation, consultezConfiguration de la journalisation pour une AWS WAF politique.
7. (Facultatif) Si vous ne souhaitez pas que certains champs et leurs valeurs soient inclus dans les journaux, censurez ces champs. Choisissez le champ à censurer, puis choisissez Ajouter. Répétez si nécessaire pour censurer des champs supplémentaires. Les champs censurés apparaîtront en tant que `REDACTED` dans les journaux. Par exemple, si vous supprimez le champ URI, le champ URI des journaux sera`REDACTED`.
8. (Facultatif) Si vous ne souhaitez pas envoyer toutes les demandes aux journaux, ajoutez vos critères de filtrage et votre comportement. Sous Filtrer les journaux, pour chaque filtre que vous souhaitez appliquer, choisissez Ajouter un filtre, puis choisissez vos critères de filtrage et indiquez si vous souhaitez conserver ou supprimer les demandes correspondant à ces critères. Lorsque vous avez fini d'ajouter des filtres, modifiez si nécessaire le comportement de journalisation par défaut. Pour plus d’informations, consultez Configuration de la journalisation des ACL Web dans le Guide du développeur AWS WAF .
9. Choisissez Suivant.
10. Vérifiez vos paramètres, puis choisissez Enregistrer pour enregistrer les modifications apportées à la politique.

Désactivation de la journalisation

La procédure suivante décrit comment désactiver la journalisation pour une AWS WAF politique dans la console Firewall Manager.

Pour désactiver la journalisation pour une AWS WAF politique

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Security Policies.
3. Choisissez la AWS WAF politique pour laquelle vous souhaitez désactiver la journalisation.
4. Dans l'onglet Détails de la politique, dans la section Règles de politique, choisissez Modifier.
5. Pour l'état de la configuration de la journalisation, choisissez Disabled.
6. Choisissez Suivant.
7. Vérifiez vos paramètres, puis choisissez Enregistrer pour enregistrer les modifications apportées à la politique.

AWS Shield Advanced politiques

Dans une AWS Shield politique de Firewall Manager, vous choisissez les ressources que vous souhaitez protéger. Lorsque vous appliquez la politique alors que la correction automatique est activée, Firewall Manager associe une ACL AWS WAF Web vide pour chaque ressource incluse qui n'est pas encore associée à une ACL AWS WAF Web. L'ACL Web vide est utilisée à des fins de surveillance du Shield. Si vous associez ensuite une autre ACL Web à la ressource, Firewall Manager supprime l'association ACL Web vide.

> **Note**
>
> Lorsqu'une ressource relevant d'une AWS WAF politique entre dans le champ d'application d'une politique Shield Advanced configurée avec une atténuation automatique des attaques DDoS au niveau de la couche application, Firewall Manager applique la protection Shield Advanced uniquement après avoir associé l'ACL Web créée par la AWS WAF politique.

Comment AWS Firewall Manager gère les ACL Web non associées dans les politiques Shield

Vous pouvez configurer si Firewall Manager gère les ACL Web non associées à votre place via le paramètre Gérer les ACL Web non associées de votre politique ou en `optimizeUnassociatedWebACLs` définissant le type de SecurityServicePolicyDatadonnées dans l'API. Si vous activez la gestion des ACL Web non associées dans votre politique, Firewall Manager crée des ACL Web dans les comptes relevant du champ d'application de la politique uniquement si les ACL Web sont utilisées par au moins une ressource. À tout moment, si un compte entre dans le champ d'application de la politique, Firewall Manager crée automatiquement une ACL Web dans le compte si au moins une ressource utilise l'ACL Web.

Lorsque vous activez la gestion des ACL Web non associées, Firewall Manager effectue un nettoyage unique des ACL Web non associées dans votre compte. Le processus de nettoyage peut prendre plusieurs heures. Si une ressource quitte le champ d'application de la politique après que Firewall Manager a créé une ACL Web, Firewall Manager ne dissocie pas la ressource de l'ACL Web. Si vous souhaitez que Firewall Manager nettoie l'ACL Web, vous devez d'abord dissocier manuellement les ressources de l'ACL Web, puis activer l'option de gestion des ACL Web non associées dans votre politique.

Si vous n'activez pas cette option, Firewall Manager ne gère pas les ACL Web non associées et Firewall Manager crée automatiquement une ACL Web dans chaque compte relevant du champ d'application de la politique.

Comment AWS Firewall Manager gère-t-il les modifications du champ d'application des politiques du Shield

Les comptes et les ressources peuvent sortir du champ d'application d'une politique AWS Firewall Manager Shield Advanced en raison d'un certain nombre de modifications, telles que la modification des paramètres du champ d'application de la politique, la modification des balises d'une ressource et

la suppression d'un compte d'une organisation. Pour des informations générales sur les paramètres du champ d'application des politiques, consultezAWS Firewall Manager portée de la politique.

Avec une politique AWS Firewall Manager Shield Advanced, si un compte ou une ressource sort de son champ d'application, Firewall Manager arrête de surveiller le compte ou la ressource.

Si un compte devient hors de portée en raison de sa suppression de l'organisation, il continuera d'être abonné à Shield Advanced. Le compte ne faisant plus partie de la famille de facturation consolidée, des frais d'abonnement à Shield Advanced seront facturés au prorata. En revanche, un compte qui sort du champ d'application mais qui reste dans l'organisation n'entraîne pas de frais supplémentaires.

Si une ressource devient hors de portée, elle continue d'être protégée par Shield Advanced et continue de faire l'objet de frais de transfert de données liés à Shield Advanced.

Atténuation automatique des attaques DDoS au niveau de

Lorsque vous appliquez une politique Shield Advanced à des CloudFront distributions Amazon ou à des équilibreurs de charge d'application, vous avez la possibilité de configurer l'atténuation automatique des attaques DDoS au niveau de la couche application de Shield Advanced dans la politique.

Pour plus d'informations sur l'atténuation automatique de Shield Advanced, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

L'atténuation automatique des attaques DDoS au niveau de la couche d'application Shield Advanced répond aux exigences suivantes :

- L'atténuation automatique des attaques DDoS au niveau de la couche application ne fonctionne qu'avec les CloudFront distributions Amazon et les équilibreurs de charge d'application.

  Si vous appliquez votre politique Shield Advanced aux CloudFront distributions Amazon, vous pouvez choisir cette option pour les politiques Shield Advanced que vous créez pour la région mondiale. Si vous appliquez des protections aux équilibreurs de charge d'application, vous pouvez appliquer la politique à toutes les régions prises en charge par Firewall Manager.
- L'atténuation automatique des attaques DDoS au niveau de la couche application fonctionne uniquement avec les ACL Web créées à l'aide de la dernière version de AWS WAF (v2).

  C'est pourquoi, si vous avez une politique qui utilise des ACL Web AWS WAF classiques, vous devez soit la remplacer par une nouvelle stratégie, qui utilisera automatiquement la dernière

version de AWS WAF, soit demander à Firewall Manager de créer une nouvelle version des ACL Web pour votre politique existante et de passer à leur utilisation. Pour plus d'informations sur ces options, consultez Remplacez les ACL Web AWS WAF classiques par les ACL Web de dernière version.

Configuration automatique des mesures d'atténuation

L'option d'atténuation automatique des attaques DDoS au niveau de la couche applicative pour les politiques Firewall Manager Shield Advanced applique la fonctionnalité d'atténuation automatique de Shield Advanced aux comptes et ressources concernés par votre politique. Pour obtenir des informations détaillées sur cette fonctionnalité Shield Advanced, consultezShield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative.

Vous pouvez choisir que Firewall Manager active ou désactive l'atténuation automatique pour les CloudFront distributions ou les équilibreurs de charge d'application concernés par la politique, ou vous pouvez choisir que la politique ignore les paramètres d'atténuation automatique de Shield Advanced :

- Activer : si vous choisissez d'activer l'atténuation automatique, vous devez également indiquer si les règles d'atténuation du Shield Advanced doivent compter ou bloquer les requêtes Web correspondantes. Firewall Manager marquera les ressources concernées comme non conformes si l'atténuation automatique n'est pas activée ou si elles utilisent une action de règle qui ne correspond pas à celle que vous spécifiez pour la politique. Si vous configurez la politique de correction automatique, Firewall Manager met à jour les ressources non conformes selon les besoins.
- Désactiver : si vous choisissez de désactiver l'atténuation automatique, Firewall Manager marquera les ressources concernées comme non conformes si l'atténuation automatique est activée. Si vous configurez la politique de correction automatique, Firewall Manager met à jour les ressources non conformes selon les besoins.
- Ignorer : si vous choisissez d'ignorer l'atténuation automatique, Firewall Manager ne tiendra compte d'aucun des paramètres d'atténuation automatique de votre politique Shield lorsqu'il effectuera des activités de correction pour cette politique. Ce paramètre vous permet de contrôler l'atténuation automatique via Shield Advanced, sans que ces paramètres ne soient remplacés par Firewall Manager. Ce paramètre ne s'applique pas aux ressources Classic Load Balancers ou Elastic IPs gérées via Shield Advanced, car Shield Advanced ne prend actuellement pas en charge l'atténuation automatique L7 pour ces ressources.

Remplacez les ACL Web AWS WAF classiques par les ACL Web de dernière version

L'atténuation automatique des attaques DDoS au niveau de la couche application fonctionne uniquement avec les ACL Web créées à l'aide de la dernière version de AWS WAF (v2).

Pour déterminer la version de l'ACL Web correspondant à votre politique Shield Advanced, consultezDéterminer la AWS WAF version utilisée par une politique Shield Advanced.

Si vous souhaitez utiliser l'atténuation automatique dans votre politique Shield Advanced et que votre politique utilise actuellement des ACL Web AWS WAF classiques, vous pouvez soit créer une nouvelle politique Shield Advanced pour remplacer votre politique Shield Advanced actuelle, soit utiliser les options décrites dans cette section pour remplacer les ACL Web des versions antérieures par de nouvelles ACL Web (v2) dans votre politique Shield Advanced actuelle. Les nouvelles politiques créent toujours des ACL Web à l'aide de la dernière version de AWS WAF. Si vous remplacez la politique dans son intégralité, vous pouvez également demander à Firewall Manager de supprimer toutes les ACL Web des versions antérieures lorsque vous la supprimez. Le reste de cette section décrit les options qui s'offrent à vous pour remplacer les ACL Web au sein de votre politique existante.

Lorsque vous modifiez une politique Shield Advanced existante pour les CloudFront ressources Amazon, Firewall Manager peut créer automatiquement une nouvelle ACL Web vide AWS WAF (v2) pour la politique, dans tout compte concerné qui ne possède pas déjà une ACL Web v2. Lorsque Firewall Manager crée une nouvelle ACL Web, si la politique possède déjà une ACL Web AWS WAF classique dans le même compte, Firewall Manager configure la nouvelle version de l'ACL Web avec le même paramètre d'action par défaut que l'ACL Web existante. S'il n'existe aucune ACL Web AWS WAF classique, Firewall Manager définit l'action par défaut sur Allow la nouvelle ACL Web. Une fois que Firewall Manager a créé une nouvelle ACL Web, vous pouvez la personnaliser selon vos besoins via la AWS WAF console.

Lorsque vous choisissez l'une des options de configuration des politiques suivantes, Firewall Manager crée de nouvelles ACL Web (v2) pour les comptes concernés qui n'en disposent pas déjà :

- Lorsque vous activez ou désactivez l'atténuation automatique des attaques DDoS au niveau de l'application. Ce choix à lui seul permet uniquement à Firewall Manager de créer les nouvelles ACL Web, et non de remplacer les associations d'ACL Web AWS WAF classiques existantes sur les ressources incluses dans le champ d'application de la politique.
- Lorsque vous choisissez l'action politique de correction automatique et que vous choisissez de remplacer les ACL Web AWS WAF classiques par des ACL Web AWS WAF (v2). Vous pouvez choisir de remplacer les ACL Web des versions antérieures, quels que soient vos choix de

configuration, pour une atténuation automatique des attaques DDoS au niveau de la couche application.

Lorsque vous choisissez l'option de remplacement, Firewall Manager crée la nouvelle version des ACL Web selon les besoins, puis effectue les opérations suivantes pour les ressources couvertes par la politique :

- Si une ressource est associée à une ACL Web issue d'une autre politique active de Firewall Manager, Firewall Manager laisse l'association tranquille.
- Dans tous les autres cas, Firewall Manager supprime toute association avec une ACL Web AWS WAF classique et associe la ressource à l'ACL Web de la politique AWS WAF (v2).

Vous pouvez choisir de demander à Firewall Manager de remplacer les ACL Web de la version précédente par les ACL Web de la nouvelle version lorsque vous le souhaitez. Si vous avez déjà personnalisé les ACL Web AWS WAF classiques de la politique, vous pouvez mettre à jour les ACL Web de la nouvelle version avec des paramètres comparables avant de demander à Firewall Manager d'effectuer l'étape de remplacement.

Vous pouvez accéder à l'une ou l'autre version de l'ACL Web pour une politique via la console de même version AWS WAF ou AWS WAF Classic.

Firewall Manager ne supprime aucune liste ACL Web AWS WAF classique remplacée tant que vous ne supprimez pas la politique elle-même. Une fois que les ACL Web AWS WAF classiques ne sont plus utilisées par la politique, vous pouvez les supprimer si vous le souhaitez.

Déterminer la AWS WAF version utilisée par une politique Shield Advanced

Vous pouvez déterminer la version de AWS WAF votre politique Firewall Manager Shield Advanced utilisée en examinant les clés de paramètres de la règle AWS Config liée aux services de la politique. Si la AWS WAF version utilisée est la plus récente, les clés de paramètre incluent `policyId` et`webAclArn`. S'il s'agit de la version précédente, AWS WAF Classic, les touches de paramètres incluent `webAclId` et`resourceTypes`.

La AWS Config règle répertorie uniquement les clés pour les ACL Web que la politique utilise actuellement avec les ressources incluses.

Pour déterminer quelle version de AWS WAF votre politique Firewall Manager Shield Advanced utilise

1. Récupérez l'ID de politique pour la politique Shield Advanced :

a. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

b. Dans le volet de navigation, sélectionnez Security Policies.

c. Choisissez la région pour la politique. Pour les CloudFront distributions, c'est le cas`Global`.

d. Recherchez la politique que vous souhaitez et copiez la valeur de son identifiant de politique.

   Exemple d'identifiant de politique :`1111111-2222-3333-4444-a55aa5aaa555`.

2. Créez le nom de la AWS Config règle de la politique en ajoutant l'ID de la politique à la chaîne`FMManagedShieldConfigRule`.

   Exemple de nom de AWS Config règle :`FMManagedShieldConfigRule1111111-2222-3333-4444-a55aa5aaa555`.

3. Recherchez les paramètres de la AWS Config règle associée pour les clés nommées `policyId` et `webAclArn` :

   a. Ouvrez la AWS Config console à l'adresse https://console.aws.amazon.com/config/.

   b. Dans le volet de navigation, choisissez Règles.

   c. Recherchez le nom de la AWS Config règle de votre politique Firewall Manager dans la liste et sélectionnez-le. La page de la règle s'ouvre.

   d. Sous Détails des règles, dans la section Paramètres, examinez les clés. Si vous trouvez des clés nommées `policyId` et`webAclArn`, la politique utilise des ACL Web créées à l'aide de la dernière version de AWS WAF. Si vous trouvez des clés nommées `webAclId` et`resourceTypes`, la politique utilise des ACL Web créées à l'aide de la version précédente, AWS WAF Classic.

Politiques des groupes de sécurité

Vous pouvez utiliser les politiques des groupes de AWS Firewall Manager sécurité pour gérer les groupes de sécurité Amazon Virtual Private Cloud pour votre organisation dans AWS Organizations. Vous pouvez appliquer des stratégies de groupe de sécurité contrôlées de manière centralisée à l'ensemble de votre organisation ou à un sous-ensemble sélectionné de vos comptes et ressources.

Vous pouvez également surveiller et gérer les stratégies de groupe de sécurité utilisées dans votre organisation, avec des stratégies de groupe de sécurité d'audit et d'utilisation.

Firewall Manager gère en permanence vos politiques et les applique aux comptes et aux ressources au fur et à mesure qu'ils sont ajoutés ou mis à jour au sein de votre organisation. Pour plus d'informations AWS Organizations, consultez le Guide de AWS Organizations l'utilisateur.

Pour plus d'informations sur les groupes de sécurité Amazon Virtual Private Cloud, consultez la section Groupes de sécurité pour votre VPC dans le guide de l'utilisateur Amazon VPC.

Vous pouvez utiliser les politiques de groupe de sécurité de Firewall Manager pour effectuer les opérations suivantes au sein de votre AWS entreprise :

- Appliquer des groupes de sécurité communs aux comptes et ressources spécifiés.
- Auditer des règles de groupe de sécurité pour rechercher et corriger les règles non conformes.
- Auditer l'utilisation des groupes de sécurité pour nettoyer les groupes de sécurité inutilisés et redondants.

Cette section décrit le fonctionnement des politiques des groupes de sécurité de Firewall Manager et fournit des conseils pour les utiliser. Pour les procédures de création de politiques de groupe de sécurité, voirCréation d'une AWS Firewall Manager politique.

Stratégies de groupe de sécurité communes

Grâce à une politique de groupe de sécurité commune, Firewall Manager fournit une association contrôlée de manière centralisée des groupes de sécurité aux comptes et aux ressources de votre entreprise. Vous spécifiez où et comment appliquer la stratégie dans votre organisation.

Vous pouvez appliquer des politiques de groupe de sécurité communes aux types de ressources suivants :

- Instance Amazon Elastic Compute Cloud (Amazon EC2)
- Interface réseau élastique
- Application Load Balancer
- Classic Load Balancer

Pour obtenir des conseils sur la création d'une politique de groupe de sécurité commune à l'aide de la console, consultezCréation d'une stratégie de groupe de sécurité commune.

VPC partagés

Dans les paramètres de la portée de la stratégie pour une stratégie de groupe de sécurité commune, vous pouvez choisir d'inclure des VPC partagés. Ce choix inclut les VPC appartenant à un autre compte et partagés avec un compte concerné. Les VPC appartenant à des comptes concernés sont toujours inclus. Pour plus d'informations sur les VPC partagés, consultez la section Travailler avec des VPC partagés dans le guide de l'utilisateur Amazon VPC.

Les mises en garde suivantes s'appliquent à l'inclusion de VPC partagés. Elles s'ajoutent aux mises en garde générales relatives aux politiques des groupes de sécurité figurant à l'adresse. Mises en garde et limites relatives à la politique des groupes de sécurité

- Firewall Manager réplique le groupe de sécurité principal dans les VPC pour chaque compte concerné. Pour un VPC partagé, Firewall Manager réplique le groupe de sécurité principal une fois pour chaque compte concerné avec lequel le VPC est partagé. Cela peut se traduire par plusieurs réplicas dans un seul VPC partagé.
- Lorsque vous créez un nouveau VPC partagé, vous ne le verrez pas représenté dans les détails de la politique de groupe de sécurité de Firewall Manager tant que vous n'aurez pas créé au moins une ressource dans le VPC relevant du champ d'application de cette stratégie.
- Lorsque vous désactivez les VPC partagés dans une politique dans laquelle les VPC partagés étaient activés, Firewall Manager supprime les répliques des groupes de sécurité qui ne sont associés à aucune ressource dans les VPC partagés. Firewall Manager laisse les groupes de sécurité répliques restants en place, mais arrête de les gérer. La suppression de ces groupes de sécurité restants nécessite une gestion manuelle dans chaque instance de VPC partagé.

Groupes de sécurité principaux

Pour chaque stratégie de groupe de sécurité commune, vous AWS Firewall Manager fournissez un ou plusieurs groupes de sécurité principaux :

- Les groupes de sécurité principaux doivent être créés par le compte administrateur de Firewall Manager et peuvent résider dans n'importe quelle instance Amazon VPC du compte.
- Vous gérez vos principaux groupes de sécurité via Amazon Virtual Private Cloud (Amazon VPC) ou Amazon Elastic Compute Cloud (Amazon EC2). Pour plus d'informations, consultez la section Travailler avec des groupes de sécurité dans le guide de l'utilisateur Amazon VPC.
- Vous pouvez nommer un ou plusieurs groupes de sécurité comme principaux pour une politique de groupe de sécurité Firewall Manager. Par défaut, le nombre de groupes de sécurité autorisés dans

une stratégie est limité à un, mais vous pouvez envoyer une demande pour augmenter cette limite. Pour plus d'informations, veuillez consulter AWS Firewall Manager quotas.

Paramètres des règles de stratégie

Vous pouvez choisir un ou plusieurs des comportements de contrôle des modifications suivants pour les groupes de sécurité et les ressources de votre stratégie de groupe de sécurité commune :

- Identifiez et signalez les modifications apportées par les utilisateurs locaux aux groupes de sécurité répliqués.
- Dissociez tous les autres groupes de sécurité des AWS ressources relevant du champ d'application de la politique.
- Distribuez les balises du groupe principal aux groupes de sécurité répliqués.

> **Important**
>
> Firewall Manager ne distribuera pas les balises système ajoutées par les AWS services dans les groupes de sécurité répliqués. Les balises système commencent par le préfixe `aws:`. En outre, Firewall Manager ne met pas à jour les balises des groupes de sécurité existants et ne crée pas de nouveaux groupes de sécurité si la politique contient des balises en conflit avec la politique de balises de l'entreprise. Pour plus d'informations sur les politiques relatives aux balises, consultez la section Politiques relatives aux balises dans le guide de AWS Organizations l'utilisateur.

- Distribuez les références aux groupes de sécurité du groupe principal aux groupes de sécurité répliqués.

  Cela vous permet d'établir facilement des règles communes de référencement des groupes de sécurité pour toutes les ressources incluses dans le champ d'application pour les instances associées au VPC du groupe de sécurité spécifié. Lorsque vous activez cette option, Firewall Manager ne propage les références aux groupes de sécurité que si les groupes de sécurité font référence à des groupes de sécurité homologues dans Amazon Virtual Private Cloud. Si les groupes de sécurité répliqués ne font pas correctement référence au groupe de sécurité homologue, Firewall Manager marque ces groupes de sécurité répliqués comme non conformes. Pour plus d'informations sur la façon de référencer les groupes de sécurité homologues dans Amazon VPC, consultez Mettre à jour vos groupes de sécurité pour référencer les groupes de sécurité homologues dans le guide d'appairage Amazon VPC.

Si vous n'activez pas cette option, Firewall Manager ne propage pas les références aux groupes de sécurité aux répliques de groupes de sécurité. Pour plus d'informations sur le peering VPC dans Amazon VPC, consultez le guide d'appairage Amazon VPC.

Création et gestion des stratégies

Lorsque vous créez votre politique de groupe de sécurité commune, Firewall Manager réplique les principaux groupes de sécurité sur chaque instance Amazon VPC comprise dans le champ d'application de la politique, et associe les groupes de sécurité répliqués aux comptes et aux ressources concernés par la politique. Lorsque vous modifiez un groupe de sécurité principal, Firewall Manager propage la modification aux répliques.

Lorsque vous supprimez une stratégie de groupe de sécurité commune, vous pouvez choisir de nettoyer les ressources créées par la stratégie. Pour les groupes de sécurité courants de Firewall Manager, ces ressources sont les répliques des groupes de sécurité. Choisissez l'option de nettoyage, sauf si vous souhaitez gérer manuellement chaque réplica après la suppression de la stratégie. Dans la plupart des situations, choisir l'option de nettoyage est l'approche la plus simple.

Mode de gestion des réplicas

Les groupes de sécurité répliqués dans les instances Amazon VPC sont gérés comme les autres groupes de sécurité Amazon VPC. Pour plus d'informations, consultez la section Groupes de sécurité pour votre VPC dans le guide de l'utilisateur Amazon VPC.

Stratégies de groupe de sécurité d'audit de contenu

Utilisez les politiques des groupes de sécurité d'audit de AWS Firewall Manager contenu pour auditer et appliquer des actions de stratégie aux règles utilisées dans les groupes de sécurité de votre organisation. Les politiques des groupes de sécurité d'audit de contenu s'appliquent à tous les groupes de sécurité créés par les clients et utilisés dans votre AWS organisation, selon le périmètre que vous définissez dans la politique.

Pour obtenir des conseils sur la création d'une politique de groupe de sécurité d'audit de contenu à l'aide de la console, consultezCréation d'une stratégie de groupe de sécurité d'audit de contenu.

Type de ressource concerné par une stratégie

Vous pouvez appliquer des politiques de groupe de sécurité d'audit de contenu aux types de ressources suivants :

- Instance Amazon Elastic Compute Cloud (Amazon EC2)
- Interface réseau élastique
- Groupe de sécurité Amazon VPC

Les groupes de sécurité sont considérés comme étant concernés par la stratégie s'ils sont explicitement dans la portée de la stratégie ou s'ils sont associés à des ressources qui sont dans la portée.

Options de règles de politique

Vous pouvez utiliser des règles de stratégie gérées ou des règles de stratégie personnalisées pour chaque stratégie d'audit de contenu, mais pas les deux.

- Règles de stratégie gérées : dans une politique comportant des règles gérées, vous pouvez utiliser des listes d'applications et de protocoles pour contrôler les règles que Firewall Manager audite et marque comme conformes ou non conformes. Vous pouvez utiliser des listes gérées par Firewall Manager. Vous pouvez également créer et utiliser vos propres listes d'applications et de protocoles. Pour plus d'informations sur ces types de listes et sur les options de gestion des listes personnalisées, consultezListes gérées.
- Règles de stratégie personnalisées : dans une politique comportant des règles de stratégie personnalisées, vous spécifiez un groupe de sécurité existant comme groupe de sécurité d'audit pour votre stratégie. Vous pouvez utiliser les règles du groupe de sécurité d'audit comme modèle qui définit les règles que Firewall Manager audite et marque comme conformes ou non conformes.

Audit des groupes de sécurité

Vous devez créer des groupes de sécurité d'audit à l'aide de votre compte administrateur Firewall Manager avant de pouvoir les utiliser dans votre politique. Vous pouvez gérer les groupes de sécurité via Amazon Virtual Private Cloud (Amazon VPC) ou Amazon Elastic Compute Cloud (Amazon EC2). Pour plus d'informations, consultez la section Travailler avec des groupes de sécurité dans le guide de l'utilisateur Amazon VPC.

Un groupe de sécurité que vous utilisez pour une stratégie de groupe de sécurité d'audit de contenu est utilisé par Firewall Manager uniquement comme référence de comparaison pour les groupes de sécurité concernés par cette stratégie. Firewall Manager ne l'associe à aucune ressource de votre organisation.

La façon dont vous définissez les règles dans le groupe de sécurité d'audit dépend de vos choix dans les paramètres des règles de politique :

- Règles de stratégie gérées : pour les paramètres des règles de stratégie gérées, vous utilisez un groupe de sécurité d'audit pour remplacer les autres paramètres de la stratégie, afin d'autoriser ou de refuser explicitement les règles qui, autrement, pourraient avoir un autre résultat de conformité.
  - Si vous choisissez de toujours autoriser les règles définies dans le groupe de sécurité d'audit, toute règle correspondant à celle définie dans le groupe de sécurité d'audit est considérée comme conforme à la stratégie, quels que soient les autres paramètres de stratégie.
  - Si vous choisissez de toujours refuser les règles définies dans le groupe de sécurité d'audit, toute règle correspondant à une règle définie dans le groupe de sécurité d'audit est considérée comme non conforme à la stratégie, quels que soient les autres paramètres de stratégie.
- Règles de stratégie personnalisées : pour les paramètres des règles de stratégie personnalisées, le groupe de sécurité d'audit fournit un exemple de ce qui est acceptable ou non acceptable dans les règles du groupe de sécurité incluses dans le champ de compétence :
  - Si vous choisissez d'autoriser l'utilisation des règles, tous les groupes de sécurité concernés ne doivent disposer que de règles se situant dans la plage autorisée par les règles de groupe de sécurité d'audit de la politique. Dans ce cas, les règles de groupe de sécurité de la politique fournissent un exemple de ce qu'il est acceptable de faire.
  - Si vous choisissez de refuser l'utilisation des règles, tous les groupes de sécurité concernés ne doivent avoir que des règles qui ne se situent pas dans la plage autorisée par les règles de groupe de sécurité d'audit de la politique. Dans ce cas, le groupe de sécurité de la politique fournit un exemple de ce qu'il n'est pas acceptable de faire.

Création et gestion des stratégies

Lorsque vous créez une stratégie de groupe de sécurité d'audit, la résolution automatique doit être désactivée. La pratique recommandée consiste à examiner les effets de la création d'une stratégie avant d'activer la résolution automatique. Après avoir examiné les effets attendus, vous pouvez modifier la stratégie et activer la résolution automatique. Lorsque la correction automatique est activée, Firewall Manager met à jour ou supprime les règles non conformes dans les groupes de sécurité concernés.

Groupes de sécurité affectés par une stratégie de groupe de sécurité d'audit

Tous les groupes de sécurité de votre organisation qui sont créés par les clients peuvent être concernés par une stratégie de groupe de sécurité d'audit.

Les groupes de sécurité de réplica ne sont pas créés par les clients et ne peuvent donc pas être directement concernés par une stratégie de groupe de sécurité d'audit. Cependant, ils peuvent être mis à jour suite à des activités de résolution automatique de la stratégie. Le groupe de sécurité principal d'une stratégie de groupe de sécurité commune est créé par le client et peut être concerné par une stratégie de groupe de sécurité d'audit. Si une politique de groupe de sécurité d'audit apporte des modifications à un groupe de sécurité principal, Firewall Manager propage automatiquement ces modifications aux répliques.

Stratégies de groupe de sécurité d'audit d'utilisation

Utilisez les politiques des groupes de sécurité AWS Firewall Manager d'audit d'utilisation pour surveiller les groupes de sécurité inutilisés et redondants dans votre organisation et éventuellement effectuer un nettoyage. Lorsque vous activez la correction automatique de cette politique, Firewall Manager effectue les opérations suivantes :

1. Consolide les groupes de sécurité redondants, si vous avez choisi cette option.
2. Supprime les groupes de sécurité non utilisés, si vous avez choisi cette option.

Vous pouvez appliquer des politiques de groupe de sécurité d'audit d'utilisation au type de ressource suivant :

- Groupe de sécurité Amazon VPC

Pour obtenir des conseils sur la création d'une politique de groupe de sécurité d'audit d'utilisation à l'aide de la console, consultezCréation d'une stratégie de groupe de sécurité d'audit d'utilisation.

Comment Firewall Manager détecte et corrige les groupes de sécurité redondants

Pour que les groupes de sécurité soient considérés comme redondants, ils doivent avoir exactement les mêmes règles définies et se trouver dans la même instance Amazon VPC.

Pour remédier à un ensemble de groupes de sécurité redondant, Firewall Manager sélectionne l'un des groupes de sécurité à conserver, puis l'associe à toutes les ressources associées aux autres groupes de sécurité de l'ensemble. Firewall Manager dissocie ensuite les autres groupes de sécurité des ressources auxquelles ils étaient associés, ce qui les rend inutilisés.

> **Note**
>
> Si vous avez également choisi de supprimer les groupes de sécurité inutilisés, Firewall Manager s'en charge ensuite. Cela peut entraîner la suppression des groupes de sécurité qui se trouvent dans l'ensemble redondant.

Comment Firewall Manager détecte et corrige les groupes de sécurité non utilisés

Firewall Manager considère qu'un groupe de sécurité n'est pas utilisé si les deux conditions suivantes sont réunies :

- Le groupe de sécurité n'est utilisé par aucune instance Amazon EC2 ou par l'interface Elastic Network Interface Amazon EC2.
- Firewall Manager n'a pas reçu d'élément de configuration correspondant dans le délai de minutes spécifié dans la période définie par les règles de politique.

La durée de la règle de politique est définie par défaut à zéro minute, mais vous pouvez l'augmenter jusqu'à 365 jours (525 600 minutes), afin de vous donner le temps d'associer de nouveaux groupes de sécurité aux ressources.

> **Important**
>
> Si vous spécifiez un nombre de minutes autre que la valeur par défaut de zéro, vous devez activer les relations indirectes dans AWS Config. Dans le cas contraire, vos politiques de groupe de sécurité d'audit d'utilisation ne fonctionneront pas comme prévu. Pour plus d'informations sur les relations indirectes dans AWS Config, voir Relations indirectes AWS Config dans le Guide du AWS Config développeur.

Firewall Manager corrige les groupes de sécurité inutilisés en les supprimant de votre compte conformément aux paramètres de vos règles, si possible. Si Firewall Manager ne parvient pas à supprimer un groupe de sécurité, il le marque comme non conforme à la politique. Firewall Manager ne peut pas supprimer un groupe de sécurité référencé par un autre groupe de sécurité.

La durée de la correction varie selon que vous utilisez le paramètre de période par défaut ou un paramètre personnalisé :

- Période définie sur zéro, valeur par défaut : avec ce paramètre, un groupe de sécurité est considéré comme inutilisé dès qu'il n'est pas utilisé par une instance Amazon EC2 ou une interface elastic network.

  Pour ce paramètre de période zéro, Firewall Manager corrige immédiatement le groupe de sécurité.
- Période supérieure à zéro — Avec ce paramètre, un groupe de sécurité est considéré comme inutilisé lorsqu'il n'est pas utilisé par une instance Amazon EC2 ou Elastic Network Interface et que Firewall Manager n'a pas reçu d'élément de configuration correspondant dans le délai spécifié.

  Pour le paramètre de période différent de zéro, Firewall Manager corrige le groupe de sécurité après qu'il soit resté inutilisé pendant 24 heures.

Spécification du compte par défaut

Lorsque vous créez une politique de groupe de sécurité d'audit d'utilisation via la console, Firewall Manager choisit automatiquement d'exclure les comptes spécifiés et d'inclure tous les autres. Le service place ensuite le compte administrateur de Firewall Manager dans la liste à exclure. Il s'agit de l'approche recommandée, qui vous permet de gérer manuellement les groupes de sécurité appartenant au compte administrateur de Firewall Manager.

Bonnes pratiques pour les stratégies de groupe de sécurité

Cette section répertorie les recommandations relatives à la gestion des groupes de sécurité à l'aide d' AWS Firewall Manager.

Exclure le compte administrateur de Firewall Manager

Lorsque vous définissez le champ d'application de la politique, excluez le compte administrateur de Firewall Manager. Lorsque vous créez une stratégie de groupe de sécurité d'audit d'utilisation via la console, il s'agit de l'option par défaut.

Désactiver le lancement avec la correction automatique

Pour les stratégies de groupe de sécurité d'audit de contenu ou d'utilisation, démarrez avec la résolution automatique désactivée. Examinez les informations détaillées de la stratégie pour déterminer les effets qu'aurait la résolution automatique aurait. Lorsque vous êtes convaincu que les modifications correspondent à vos souhaits, modifiez la stratégie pour activer la résolution automatique.

Éviter les conflits en cas d'utilisation de sources externes pour gérer des groupes de sécurité

Si vous utilisez un outil ou un service autre que Firewall Manager pour gérer les groupes de sécurité, veillez à éviter les conflits entre les paramètres de Firewall Manager et ceux de votre source externe. Si vous avez recours à la correction automatique et que vos paramètres se contredisent, vous pouvez créer un cycle de résolution sans fin qui consomme des ressources des deux côtés.

Supposons, par exemple, que vous configuriez un autre service pour gérer un groupe de sécurité pour un ensemble de AWS ressources, et que vous configuriez une politique de Firewall Manager afin de maintenir un groupe de sécurité différent pour certaines ou toutes les mêmes ressources. Si vous configurez l'un des deux services pour interdire l'association d'un autre groupe de sécurité aux ressources concernées, celui-ci supprimera l'association de ce groupe de sécurité dans l'autre service. Si les deux services sont configurés de cette manière, vous pouvez vous retrouver avec un cycle de désassociations et d'associations sans fin.

Supposons également que vous créiez une politique d'audit de Firewall Manager pour appliquer une configuration de groupe de sécurité en conflit avec la configuration de groupe de sécurité de l'autre service. Les mesures correctives appliquées par la politique d'audit de Firewall Manager peuvent mettre à jour ou supprimer ce groupe de sécurité, le rendant ainsi non conforme pour l'autre service. Si l'autre service est configuré pour surveiller et résoudre automatiquement les problèmes détectés, il recréera ou mettra à jour le groupe de sécurité, le rendant ainsi non conforme à la politique d'audit de Firewall Manager. Si la politique d'audit de Firewall Manager est configurée avec une correction automatique, elle met à jour ou supprime à nouveau le groupe de sécurité externe, etc.

Pour éviter de tels conflits, créez des configurations qui s'excluent mutuellement entre Firewall Manager et toute source externe.

Vous pouvez utiliser le balisage pour exclure les groupes de sécurité extérieurs de la correction automatique prévue par vos politiques de Firewall Manager. Pour ce faire, ajoutez une ou plusieurs balises aux groupes de sécurité ou à d'autres ressources gérées par la source externe. Ensuite, lorsque vous définissez le champ d'application de la politique de Firewall Manager, dans la spécification de vos ressources, excluez les ressources qui possèdent le ou les tags que vous avez ajoutés.

De même, dans votre outil ou service externe, excluez les groupes de sécurité gérés par Firewall Manager de toute activité de gestion ou d'audit. N'importez pas les ressources de Firewall Manager ou utilisez le balisage spécifique à Firewall Manager pour les exclure de la gestion externe.

Bonnes pratiques en matière d'audit d'utilisation, politiques de groupe de sécurité

Suivez ces directives lorsque vous utilisez des politiques de groupe de sécurité d'audit d'utilisation.

- Évitez de modifier plusieurs fois le statut d'association d'un groupe de sécurité dans un court laps de temps, par exemple dans un délai de 15 minutes. Cela peut empêcher Firewall Manager de rater certains ou tous les événements correspondants. Par exemple, n'associez et ne dissociez pas rapidement un groupe de sécurité à une interface elastic network.

Mises en garde et limites relatives à la politique des groupes de sécurité

Cette section répertorie les mises en garde et les limites liées à l'utilisation des politiques de groupe de sécurité de Firewall Manager :

- La mise à jour des groupes de sécurité pour les interfaces réseau élastiques Amazon EC2 créées à l'aide du type de service Fargate n'est pas prise en charge. Vous pouvez toutefois mettre à jour les groupes de sécurité pour les interfaces réseau élastiques Amazon ECS avec le type de service Amazon EC2.
- Firewall Manager ne prend pas en charge les groupes de sécurité pour les interfaces réseau élastiques Amazon EC2 créées par Amazon Relational Database Service.
- La mise à jour des interfaces réseau élastiques Amazon ECS n'est possible que pour les services Amazon ECS qui utilisent le contrôleur de déploiement de mise à jour continue (Amazon ECS). Pour les autres contrôleurs de déploiement Amazon ECS tels que CODE_DEPLOY ou les contrôleurs externes, Firewall Manager ne peut actuellement pas mettre à jour les interfaces réseau élastiques.
- Avec les groupes de sécurité pour les interfaces réseau élastiques Amazon EC2, les modifications apportées à un groupe de sécurité ne sont pas immédiatement visibles par Firewall Manager. Firewall Manager détecte généralement les modifications en quelques heures, mais la détection peut être retardée jusqu'à six heures.
- Firewall Manager ne prend pas en charge la mise à jour des groupes de sécurité dans les interfaces réseau élastiques pour les Network Load Balancers.
- Dans les politiques de groupe de sécurité courantes, si un VPC partagé est ultérieurement départagé avec un compte, Firewall Manager ne supprimera pas les répliques de groupes de sécurité du compte.
- Avec les politiques de groupe de sécurité d'audit d'utilisation, si vous créez plusieurs politiques avec un paramètre de délai personnalisé qui ont toutes le même champ d'application, la première stratégie contenant des résultats de conformité sera celle qui communique les résultats.

Cas d'utilisation des stratégies de groupe de sécurité

Vous pouvez utiliser des politiques de groupe de sécurité AWS Firewall Manager communes pour automatiser la configuration du pare-feu hôte pour les communications entre les instances Amazon VPC. Cette section répertorie les architectures Amazon VPC standard et décrit comment les sécuriser à l'aide des politiques de groupe de sécurité communes de Firewall Manager. Ces politiques de groupe de sécurité peuvent vous aider à appliquer un ensemble unifié de règles pour sélectionner les ressources de différents comptes et à éviter les configurations par compte dans Amazon Elastic Compute Cloud et Amazon VPC.

Grâce aux politiques de groupe de sécurité communes de Firewall Manager, vous pouvez étiqueter uniquement les interfaces réseau élastiques EC2 dont vous avez besoin pour communiquer avec les instances d'un autre Amazon VPC. Les autres instances du même Amazon VPC sont alors plus sécurisées et isolées.

Cas d'utilisation : surveillance et contrôle des demandes adressées aux équilibreurs de charge d'application et aux équilibreurs de charge classiques

Vous pouvez utiliser une politique de groupe de sécurité commune de Firewall Manager pour définir les demandes que vos équilibreurs de charge intégrés doivent traiter. Vous pouvez le configurer via la console Firewall Manager. Seules les demandes conformes aux règles entrantes du groupe de sécurité peuvent atteindre vos équilibreurs de charge, et les équilibreurs de charge distribueront uniquement les demandes conformes aux règles sortantes.

Cas d'utilisation : Amazon VPC public et accessible par Internet

Vous pouvez utiliser une politique de groupe de sécurité commune de Firewall Manager pour sécuriser un Amazon VPC public, par exemple, afin d'autoriser uniquement le port entrant 443. Cela revient au même que d'autoriser uniquement le trafic HTTPS entrant pour un VPC public. Vous pouvez étiqueter les ressources publiques au sein du VPC (par exemple, en tant que « PublicVPC »), puis définir le champ d'application de la politique de Firewall Manager de manière à ce que seules les ressources dotées de cette balise soient définies. Firewall Manager applique automatiquement la politique à ces ressources.

Cas d'utilisation : instances Amazon VPC publiques et privées

Vous pouvez utiliser la même politique de groupe de sécurité commune pour les ressources publiques que celle recommandée dans le cas d'utilisation précédent pour les instances publiques Amazon VPC accessibles sur Internet. Vous pouvez utiliser une deuxième stratégie de groupe de

sécurité commune pour limiter la communication entre les ressources publiques et les ressources privées. Marquez les ressources des instances Amazon VPC publiques et privées avec quelque chose comme « PublicPrivate » pour leur appliquer la deuxième politique. Vous pouvez utiliser une troisième politique pour définir la communication autorisée entre les ressources privées et d'autres instances privées ou privées d'Amazon VPC. Pour cette stratégie, vous pouvez utiliser une autre balise d'identification sur les ressources privées.

Cas d'utilisation : instances Amazon VPC Hub and Spoke

Vous pouvez utiliser une politique de groupe de sécurité commune pour définir les communications entre l'instance Amazon VPC hub et les instances Amazon VPC parlées. Vous pouvez utiliser une deuxième politique pour définir la communication entre chaque instance Amazon VPC en étoile et l'instance Amazon VPC du hub.

Cas d'utilisation : interface réseau par défaut pour les instances Amazon EC2

Vous pouvez utiliser une stratégie de groupe de sécurité commune pour autoriser uniquement les communications standard, par exemple les services SSH et de mise à jour de correctif/système d'exploitation internes, et pour interdire d'autres communications non sécurisées.

Cas d'utilisation : identifier les ressources avec des autorisations ouvertes

Vous pouvez utiliser une stratégie de groupe de sécurité d'audit pour identifier toutes les ressources de votre organisation qui sont autorisées à communiquer avec des adresses IP publiques ou qui possèdent des adresses IP appartenant à des fournisseurs tiers.

Politiques relatives à la liste de contrôle d'accès réseau (ACL) Amazon VPC

Cette section décrit le fonctionnement des politiques ACL du AWS Firewall Manager réseau et fournit des conseils pour les utiliser. Pour obtenir des conseils sur la création d'une politique ACL réseau à l'aide de la console, reportez-vous àCréation d'une politique ACL réseau.

Pour plus d'informations sur les listes de contrôle d'accès réseau (ACL) Amazon VPC, consultez la section Contrôler le trafic vers les sous-réseaux à l'aide des listes ACL réseau dans le guide de l'utilisateur Amazon VPC.

Vous pouvez utiliser les politiques ACL du réseau Firewall Manager pour gérer les listes de contrôle d'accès réseau (ACL) Amazon Virtual Private Cloud (Amazon VPC) pour votre organisation dans. AWS Organizations Vous définissez les paramètres des règles ACL réseau de la politique ainsi que les comptes et sous-réseaux auxquels vous souhaitez que les paramètres soient appliqués.

Firewall Manager applique en permanence vos paramètres de politique aux comptes et aux sous-réseaux au fur et à mesure qu'ils sont ajoutés ou mis à jour au sein de votre organisation. Pour plus d'informations sur le champ d'application de la politique AWS Firewall Manager portée de la politique et consultez le Guide de AWS Organizations l'utilisateur. AWS Organizations

Lorsque vous définissez une politique ACL réseau Firewall Manager, outre les paramètres de stratégie standard de Firewall Manager, tels que le nom et la portée, vous fournissez les informations suivantes :

- Première et dernière règles de gestion du trafic entrant et sortant. Firewall Manager impose leur présence et leur ordre dans les listes de contrôle d'accès du réseau couvertes par la politique, ou signale les cas de non-conformité. Vos comptes individuels peuvent créer des règles personnalisées à appliquer entre la première et la dernière règle de la politique.
- S'il faut forcer la correction lorsque la correction entraînerait des conflits de gestion du trafic entre les règles de l'ACL du réseau. Cela s'applique uniquement lorsque la correction est activée pour la politique.

Règles ACL et balisage du réseau Firewall Manager

Cette section décrit les spécifications des règles de politique ACL réseau et les ACL réseau gérées par Firewall Manager.

Marquage sur un réseau géré ACL

Firewall Manager étiquette une ACL de réseau géré avec une `FMManaged` balise dont la valeur est de`true`. Firewall Manager effectue des corrections uniquement sur les ACL réseau dotées de ce paramètre de balise.

Règles que vous définissez dans la politique

Dans la spécification de votre politique ACL réseau, vous définissez les règles que vous souhaitez exécuter en premier et en dernier pour le trafic entrant et les règles que vous souhaitez exécuter en premier et en dernier pour le trafic sortant.

Par défaut, vous pouvez définir jusqu'à 5 règles entrantes, à utiliser dans n'importe quelle combinaison des premières et dernières règles de la politique. De même, vous pouvez définir jusqu'à 5 règles de sortie. Pour en savoir plus sur ces limites, consultezQuotas souples. Pour plus d'informations sur les limites générales des ACL réseau, consultez les quotas Amazon VPC sur les ACL réseau dans le guide de l'utilisateur Amazon VPC.

Vous n'attribuez pas de numéros de règles aux règles de politique. Au lieu de cela, vous spécifiez les règles dans l'ordre dans lequel vous souhaitez qu'elles soient évaluées, et Firewall Manager utilise cet ordre pour attribuer des numéros de règles dans les ACL du réseau qu'il gère.

En outre, vous gérez les spécifications des règles ACL réseau de la politique comme vous le feriez pour les règles d'une ACL réseau via Amazon VPC. Pour plus d'informations sur la gestion des ACL réseau dans Amazon VPC, consultez les sections Contrôler le trafic vers les sous-réseaux à l'aide des ACL réseau et Travailler avec des ACL réseau dans le guide de l'utilisateur Amazon VPC.

Règles dans un réseau géré ACL

Firewall Manager configure les règles d'une ACL réseau qu'il gère en plaçant les premières et dernières règles de la politique avant et après les règles personnalisées définies par un responsable de compte individuel. Firewall Manager préserve l'ordre des règles personnalisées. Les ACL du réseau sont évaluées en commençant par la règle du numéro le plus bas.

Lorsque Firewall Manager crée pour la première fois une ACL réseau, il définit les règles avec la numérotation suivante :

- Premières règles : 1, 2,... — Défini par vos soins dans la politique ACL du réseau Firewall Manager.

  Firewall Manager attribue des numéros de règles commençant à 1 par incréments de 1, les règles étant ordonnées comme vous les avez ordonnées dans la spécification de la politique.
- Règles personnalisées : 5 000, 5 100,... — Géré par des responsables de comptes individuels via Amazon VPC.

  Firewall Manager attribue des numéros à ces règles en commençant par 5 000 et en augmentant de 100 pour chaque règle suivante.
- Dernières règles :... 32 765, 32 766 — Défini par vous dans la politique ACL du réseau Firewall Manager.

  Firewall Manager attribue des numéros de règles qui se terminent par le nombre le plus élevé possible, 32766 par incréments de 1, les règles étant ordonnées comme vous les avez ordonnées dans la spécification de la politique.

Après l'initialisation des ACL réseau, Firewall Manager ne contrôle pas les modifications apportées par les comptes individuels dans ses ACL réseau gérées. Les comptes individuels peuvent modifier une ACL réseau sans la rendre non conforme, à condition que les règles personnalisées restent

numérotées entre la première et la dernière règle de la politique, et que les première et dernière règles conservent leur ordre spécifié. Il est recommandé de respecter la numérotation décrite dans cette section lors de la gestion des règles personnalisées.

Comment Firewall Manager initie la gestion des ACL réseau pour un sous-réseau

Firewall Manager commence à gérer l'ACL réseau pour un sous-réseau lorsqu'il associe le sous-réseau à une ACL réseau que Firewall Manager a créée et étiquetée avec `FMManaged` set to. `true`

La conformité à une politique d'ACL réseau nécessite que les premières règles de la stratégie soient positionnées en premier, dans l'ordre spécifié dans la politique, les dernières règles positionnées en dernier, dans l'ordre, et toutes les autres règles personnalisées positionnées au milieu. Ces exigences peuvent être satisfaites par une ACL réseau non gérée à laquelle le sous-réseau est déjà associé ou par une ACL réseau gérée.

Lorsque Firewall Manager applique une politique ACL réseau à un sous-réseau associé à une ACL réseau non gérée, Firewall Manager vérifie les points suivants dans l'ordre et s'arrête lorsqu'il identifie une option viable :

1. L'ACL réseau associée est déjà conforme : si l'ACL réseau actuellement associée au sous-réseau est conforme, Firewall Manager laisse cette association en place et ne démarre pas la gestion des ACL réseau pour le sous-réseau.

   Firewall Manager ne modifie ni ne gère une ACL réseau dont il n'est pas le propriétaire, mais tant qu'elle est conforme, Firewall Manager la laisse en place et surveille simplement sa conformité aux politiques.
2. Un ACL réseau géré conforme est disponible : si Firewall Manager gère déjà un ACL réseau conforme à la configuration requise, c'est une option. Si la correction est activée, Firewall Manager y associe le sous-réseau. Si la correction est désactivée, Firewall Manager marque le sous-réseau comme non conforme et propose le remplacement de l'association ACL réseau comme option de correction.
3. Création d'une nouvelle ACL réseau gérée conforme : si la correction est activée, Firewall Manager crée une nouvelle ACL réseau et l'associe au sous-réseau. Dans le cas contraire, Firewall Manager marque le sous-réseau comme non conforme et propose les options de correction consistant à créer la nouvelle ACL réseau et à remplacer l'association ACL réseau.

Si ces étapes échouent, Firewall Manager signale la non-conformité du sous-réseau.

Firewall Manager suit ces étapes lorsqu'un sous-réseau entre pour la première fois dans le champ d'application et lorsque l'ACL réseau non géré d'un sous-réseau n'est pas conforme.

Comment Firewall Manager remédie aux ACL non conformes des réseaux gérés

Cette section décrit comment Firewall Manager corrige les ACL de son réseau géré lorsqu'elles ne sont pas conformes à la politique. Firewall Manager corrige uniquement les ACL du réseau géré, avec la balise définie sur`FMManaged`. `true` Pour les ACL réseau qui ne sont pas gérées par Firewall Manager, consultezGestion initiale des ACL du réseau.

La correction rétablit les emplacements relatifs des premières règles, des règles personnalisées et des dernières règles et rétablit l'ordre des premières et des dernières règles. Au cours de la correction, Firewall Manager ne déplace pas nécessairement les règles vers les numéros de règles qu'il utilise lors de l'initialisation des ACL réseau. Pour les paramètres numériques initiaux et les descriptions de ces catégories de règles, consultezGestion initiale des ACL du réseau.

Afin d'établir des règles conformes et un ordre des règles, Firewall Manager peut avoir besoin de déplacer les règles au sein de l'ACL du réseau. Firewall Manager préserve autant que possible les protections de l'ACL du réseau en maintenant l'ordre des règles conformes existant. Par exemple, il peut dupliquer temporairement les règles vers de nouveaux emplacements, puis effectuer une suppression ordonnée des règles d'origine, en préservant les emplacements relatifs pendant le processus.

Cette approche protège vos paramètres, mais elle nécessite également de l'espace dans l'ACL du réseau pour les règles provisoires. Si Firewall Manager atteint le nombre limite de règles dans une ACL réseau, il interrompt la correction. Dans ce cas, l'ACL du réseau n'est toujours pas conforme et Firewall Manager indique la raison.

Si un compte ajoute des règles personnalisées à une ACL réseau gérée par Firewall Manager et que ces règles interfèrent avec la correction de Firewall Manager, Firewall Manager arrête toute activité de correction sur l'ACL réseau et signale le conflit.

Assainissement forcé

Si vous choisissez la correction automatique pour la politique, vous spécifiez également si vous souhaitez forcer la correction pour les premières règles ou pour les dernières règles.

Lorsque Firewall Manager rencontre un conflit dans la gestion du trafic entre une règle personnalisée et une règle de politique, il fait référence au paramètre de correction forcée correspondant. Si la

correction forcée est activée, Firewall Manager applique la correction, malgré le conflit. Si cette option n'est pas activée, Firewall Manager arrête la correction. Dans les deux cas, Firewall Manager signale le conflit de règles et propose des options de correction.

Exigences et limites relatives au nombre de règles

Au cours de la correction, Firewall Manager peut temporairement dupliquer les règles afin de les déplacer sans altérer les protections qu'elles fournissent.

Pour les règles entrantes ou sortantes, le plus grand nombre de règles dont Firewall Manager peut avoir besoin pour effectuer la correction est le suivant :

```
2 * (the number of rules defined in the policy for the traffic direction)
+
the number of custom rules defined in the network ACL for the traffic direction
```

Les ACL réseau et les politiques ACL réseau sont soumises à des limites de règles modifiables. Si Firewall Manager atteint une limite dans ses efforts de correction, il arrête d'essayer de remédier et signale la non-conformité.

Pour permettre à Firewall Manager d'effectuer ses activités de correction, vous pouvez demander une augmentation de la limite. Vous pouvez également modifier la configuration de la politique ou de l'ACL réseau afin de réduire le nombre de règles utilisées.

Pour plus d'informations sur les limites d'ACL du réseau, consultez les quotas Amazon VPC sur les ACL du réseau dans le guide de l'utilisateur Amazon VPC.

En cas d'échec de la correction

Lors de la mise à jour d'une ACL réseau, si Firewall Manager doit s'arrêter pour une raison quelconque, il n'annule pas les modifications, mais laisse l'ACL réseau dans un état provisoire. Si vous constatez des règles dupliquées dans une ACL réseau dont la `FMManaged` balise est définie sur`true`, Firewall Manager est probablement en train de la corriger. Les modifications peuvent être partiellement achevées pendant un certain temps, mais en raison de l'approche adoptée par Firewall Manager en matière de correction, cela n'interrompra pas le trafic et ne réduira pas la protection des sous-réseaux associés.

Lorsque Firewall Manager ne corrige pas complètement les ACL réseau non conformes, il signale la non-conformité des sous-réseaux associés et suggère des options de correction possibles.

Réessayer en cas d'échec de la correction

Dans la plupart des cas, si Firewall Manager ne parvient pas à effectuer les modifications correctives apportées à une ACL réseau, il réessaiera éventuellement de le faire.

L'exception à cette règle est lorsque la correction atteint la limite du nombre de règles ACL du réseau ou la limite du nombre d'ACL du réseau VPC. Firewall Manager ne peut pas effectuer d'activités de correction qui privent AWS les ressources de leurs paramètres limites. Dans ces cas, vous devez réduire le nombre ou augmenter les limites pour pouvoir continuer. Pour plus d'informations sur les limites, consultez les quotas Amazon VPC sur les ACL réseau dans le guide de l'utilisateur Amazon VPC.

Rapports de conformité aux ACL du réseau Firewall Manager

Firewall Manager surveille et signale la conformité de toutes les ACL réseau associées aux sous-réseaux concernés.

D'une manière générale, la non-conformité se produit dans des situations telles que l'ordre incorrect des règles ou un conflit dans le comportement de gestion du trafic entre les règles politiques et les règles personnalisées. Les rapports de non-conformité incluent les violations de conformité et les options de correction.

Firewall Manager signale les violations de conformité pour une politique ACL réseau de la même manière que pour les autres types de politiques. Pour plus d'informations sur les rapports de conformité, consultezAfficher les informations de conformité d'une AWS Firewall Manager politique.

Non-conformité lors des mises à jour des politiques

Une fois que vous avez modifié une politique ACL réseau, jusqu'à ce que Firewall Manager mette à jour les ACL réseau couvertes par la politique, Firewall Manager marque ces ACL réseau comme non conformes. Firewall Manager le fait même si les ACL du réseau peuvent, à proprement parler, être conformes.

Par exemple, si vous supprimez des règles de la spécification de stratégie, alors que les ACL du réseau concernées contiennent toujours des règles supplémentaires, leurs définitions de règles peuvent toujours être conformes à la politique. Cependant, étant donné que les règles supplémentaires font partie des règles gérées par Firewall Manager, Firewall Manager les considère comme des violations des paramètres de politique actuels. Cela est différent de la façon dont Firewall Manager affiche les règles personnalisées que vous ajoutez aux listes de contrôle d'accès du réseau géré par Firewall Manager.

Bonnes pratiques d'utilisation des politiques ACL du réseau Firewall Manager

Cette section répertorie les recommandations relatives à l'utilisation des politiques ACL du réseau Firewall Manager et des ACL du réseau géré.

Reportez-vous à la **`FMManaged`** balise pour identifier les ACL réseau gérées par Firewall Manager

Les ACL réseau gérées par Firewall Manager ont la `FMManaged` balise définie sur. `true` Utilisez cette balise pour vous aider à distinguer vos propres ACL réseau personnalisées de celles que vous gérez via Firewall Manager.

Ne modifiez pas la valeur de la **`FMManaged`** balise sur une ACL réseau

Firewall Manager utilise cette balise pour définir et déterminer son état de gestion à l'aide d'une ACL réseau.

Ne modifiez pas les associations pour les sous-réseaux dotés de listes de contrôle d'accès réseau gérées par Firewall Manager

Ne modifiez pas manuellement les associations entre vos sous-réseaux et les ACL réseau gérées par Firewall Manager. Cela peut empêcher Firewall Manager de gérer les protections de ces sous-réseaux. Vous pouvez identifier les ACL réseau qui sont gérées par Firewall Manager en recherchant les paramètres de `FMManaged` balise de`true`.

Pour supprimer un sous-réseau de la gestion des politiques de Firewall Manager, utilisez les paramètres de portée des politiques de Firewall Manager pour exclure le sous-réseau. Par exemple, vous pouvez étiqueter le sous-réseau, puis exclure cette balise du champ d'application de la politique. Pour plus d’informations, consultez AWS Firewall Manager portée de la politique.

Lorsque vous mettez à jour une ACL réseau gérée, ne modifiez pas les règles gérées par Firewall Manager

Dans une ACL réseau gérée par Firewall Manager, séparez vos règles personnalisées des règles politiques en respectant le schéma de numérotation décrit dans. Règles ACL et balisage du réseau Firewall Manager Ajoutez ou modifiez uniquement les règles dont les nombres sont compris entre 5 000 et 32 000.

Évitez d'ajouter trop de règles pour les limites de votre compte

Lors de la correction d'un ACL réseau, Firewall Manager augmente généralement le nombre de règles ACL du réseau temporairement. Pour éviter les problèmes de non-conformité, assurez-vous

de disposer de suffisamment de place pour les règles que vous utilisez. Pour plus d'informations, consultez Comment Firewall Manager remédie aux ACL non conformes des réseaux gérés.

Désactiver le lancement avec la correction automatique

Commencez par désactiver la correction automatique, puis passez en revue les informations détaillées de la politique pour déterminer les effets que la correction automatique aurait. Lorsque vous êtes convaincu que les modifications correspondent à vos souhaits, modifiez la stratégie pour activer la résolution automatique.

Mises en garde relatives à la politique ACL du réseau Firewall Manager

Cette section répertorie les mises en garde et les limites liées à l'utilisation des politiques ACL du réseau Firewall Manager.

- Temps de mise à jour plus lent qu'avec les autres politiques : Firewall Manager applique généralement les politiques ACL du réseau et modifie les politiques plus lentement qu'avec les autres politiques de Firewall Manager, en raison des limites de la vitesse à laquelle les API ACL du réseau Amazon EC2 sont capables de traiter les demandes. Vous remarquerez peut-être que les modifications de politique prennent plus de temps que les modifications similaires apportées aux autres politiques de Firewall Manager, en particulier lorsque vous ajoutez une politique pour la première fois.
- Pour la protection initiale des sous-réseaux, Firewall Manager préfère les anciennes politiques. Cela s'applique uniquement aux sous-réseaux qui ne sont pas encore protégés par une politique ACL du réseau Firewall Manager. Si un sous-réseau entre dans le champ d'application de plusieurs politiques ACL en même temps, Firewall Manager utilise la plus ancienne stratégie pour protéger le sous-réseau.
- Raisons pour lesquelles une politique cesse de protéger un sous-réseau — Une politique qui gère l'ACL réseau pour un sous-réseau conserve la gestion jusqu'à ce que l'une des situations suivantes se produise :
  - Le sous-réseau sort du champ d'application de la politique.
  - La politique est supprimée.
  - Vous modifiez manuellement l'association du sous-réseau en une ACL réseau gérée par une politique de Firewall Manager différente et pour laquelle le sous-réseau est concerné.

Suppression d'une politique ACL du réseau Firewall Manager

Lorsque vous supprimez une politique ACL réseau de Firewall Manager, Firewall Manager remplace les valeurs des `FMManaged` balises par `false` des valeurs correspondant à toutes les ACL réseau qu'il gère pour cette politique.

En outre, vous pouvez choisir de nettoyer ou non les ressources créées par la politique. Si vous choisissez le nettoyage, Firewall Manager essaie de suivre les étapes suivantes dans l'ordre :

1. Restaurez l'association d'origine : Firewall Manager essaie de réassocier le sous-réseau à l'ACL réseau à laquelle il était associé avant que Firewall Manager ne commence à le gérer.
2. Supprimer les premières et dernières règles de l'ACL réseau : s'il ne parvient pas à modifier l'association, Firewall Manager essaie de supprimer les premières et dernières règles de la politique, en ne laissant que les règles personnalisées dans l'ACL réseau associée au sous-réseau.
3. Ne rien modifier aux règles ou à l'association : s'il ne peut effectuer aucune des actions ci-dessus, Firewall Manager laisse l'ACL réseau et son association inchangées.

Si vous ne choisissez pas l'option de nettoyage, vous devrez gérer manuellement chaque ACL réseau après la suppression de la politique. Dans la plupart des situations, choisir l'option de nettoyage est l'approche la plus simple.

AWS Network Firewall politiques

Vous pouvez utiliser les politiques de AWS Firewall Manager Network Firewall pour gérer AWS Network Firewall les pare-feux de vos Amazon Virtual Private Cloud VPC au sein de votre organisation dans. AWS Organizations Vous pouvez appliquer des pare-feux contrôlés de manière centralisée à l'ensemble de votre organisation ou à un sous-ensemble sélectionné de vos comptes et VPC.

Network Firewall fournit des protections de filtrage du trafic réseau pour les sous-réseaux publics de vos VPC. Firewall Manager crée et gère vos pare-feux en fonction du type de gestion de pare-feu défini par votre politique. Firewall Manager propose les modèles de gestion de pare-feu suivants :

- Distribué : pour chaque compte et VPC relevant du champ d'application des politiques, Firewall Manager crée un pare-feu Network Firewall et déploie les points de terminaison du pare-feu sur les sous-réseaux VPC afin de filtrer le trafic réseau.

- Centralisé : Firewall Manager crée un pare-feu Network Firewall unique dans un seul Amazon VPC.
- Importer des pare-feux existants : Firewall Manager importe les pare-feux existants à des fins de gestion dans le cadre d'une politique Firewall Manager unique. Vous pouvez appliquer des règles supplémentaires aux pare-feux importés gérés par votre politique afin de garantir qu'ils répondent à vos normes de sécurité.

> **Note**
>
> Les politiques de Firewall Manager Network Firewall sont des politiques de Firewall Manager que vous utilisez pour gérer les protections Network Firewall de vos VPC au sein de votre organisation.
> Les protections du Network Firewall sont spécifiées dans les ressources du service Network Firewall appelées politiques de pare-feu.

Pour plus d'informations sur l'utilisation de Network Firewall, consultez le manuel du AWS Network Firewall développeur.

Les sections suivantes décrivent les conditions requises pour utiliser les politiques de Firewall Manager Network Firewall et décrivent le fonctionnement de ces politiques. Pour la procédure de création de la politique, voirCréation d'une AWS Firewall Manager politique pour AWS Network Firewall.

Vous devez activer le partage des ressources

Une politique de Network Firewall partage les groupes de règles du Network Firewall entre les comptes de votre organisation. Pour que cela fonctionne, le partage des ressources doit être activé pour AWS Organizations. Pour plus d'informations sur la façon d'activer le partage des ressources, consultezPartage des ressources pour les politiques de Network Firewall et de DNS Firewall.

Les groupes de règles de votre Network Firewall doivent être définis

Lorsque vous spécifiez une nouvelle politique de Network Firewall, vous la définissez de la même manière que lorsque vous l'utilisez AWS Network Firewall directement. Vous spécifiez les groupes de règles apatrides à ajouter, les actions apatrides par défaut et les groupes de règles apatrides. Vos groupes de règles doivent déjà exister dans le compte administrateur de Firewall Manager pour que

vous puissiez les inclure dans la politique. Pour plus d'informations sur la création de groupes de règles Network Firewall, consultez la section Groupes de AWS Network Firewall règles.

Comment Firewall Manager crée les points de terminaison du pare-feu

Le type de gestion de pare-feu indiqué dans votre politique détermine la manière dont Firewall Manager crée les pare-feux. Votre politique peut créer des pare-feux distribués, un pare-feu centralisé ou vous pouvez importer des pare-feux existants :

- Distribué : avec le modèle de déploiement distribué, Firewall Manager crée des points de terminaison pour chaque VPC relevant du champ d'application de la politique. Vous pouvez soit personnaliser l'emplacement du point de terminaison en spécifiant les zones de disponibilité dans lesquelles créer des points de terminaison de pare-feu, soit Firewall Manager peut créer automatiquement des points de terminaison dans les zones de disponibilité avec des sous-réseaux publics. Si vous choisissez manuellement les zones de disponibilité, vous avez la possibilité de restreindre l'ensemble des CIDR autorisés par zone de disponibilité. Si vous décidez de laisser Firewall Manager créer automatiquement les points de terminaison, vous devez également spécifier si le service créera un point de terminaison unique ou plusieurs points de terminaison de pare-feu au sein de vos VPC.
  - Pour plusieurs points de terminaison de pare-feu, Firewall Manager déploie un point de terminaison de pare-feu dans chaque zone de disponibilité où vous avez un sous-réseau avec une passerelle Internet ou un itinéraire de point de terminaison de pare-feu créé par Firewall Manager dans la table de routage. Il s'agit de l'option par défaut pour une politique Network Firewall.
  - Pour un point de terminaison de pare-feu unique, Firewall Manager déploie un point de terminaison de pare-feu dans une seule zone de disponibilité de tout sous-réseau doté d'un itinéraire de passerelle Internet. Avec cette option, le trafic dans les autres zones doit franchir les limites des zones pour être filtré par le pare-feu.

    > **Note**
    >
    > Pour ces deux options, un sous-réseau doit être associé à une table de routage contenant une route IPv4/PrefixList. Firewall Manager ne recherche aucune autre ressource.

- Centralisé : avec le modèle de déploiement centralisé, Firewall Manager crée un ou plusieurs points de terminaison de pare-feu au sein d'un VPC d'inspection. Un VPC d'inspection est un VPC central dans lequel Firewall Manager lance vos points de terminaison. Lorsque vous utilisez

le modèle de déploiement centralisé, vous spécifiez également les zones de disponibilité dans lesquelles créer les points de terminaison du pare-feu. Vous ne pouvez pas modifier le VPC d'inspection après avoir créé votre politique. Pour utiliser un autre VPC d'inspection, vous devez créer une nouvelle politique.

- Importer des pare-feux existants : lorsque vous importez des pare-feux existants, vous choisissez les pare-feux à gérer dans votre politique en ajoutant un ou plusieurs ensembles de ressources à votre politique. Un ensemble de ressources est un ensemble de ressources, en l'occurrence des pare-feux existants dans Network Firewall, qui sont gérés par un compte au sein de votre organisation. Avant d'utiliser des ensembles de ressources dans votre politique, vous devez d'abord créer un ensemble de ressources. Pour plus d'informations sur les ensembles de ressources de Firewall Manager, consultezUtilisation des ensembles de ressources dans Firewall Manager.

  Tenez compte des considérations suivantes lorsque vous utilisez des pare-feux importés :

  - Si un pare-feu importé devient non conforme, Firewall Manager essaiera de résoudre automatiquement la violation, sauf dans les cas suivants :
    - En cas de discordance entre les actions par défaut avec ou sans état de la politique de Firewall Firewall définies dans le Firewall Manager.
    - Si un groupe de règles de la politique de pare-feu d'un pare-feu importé a la même priorité qu'un groupe de règles de la stratégie Firewall Manager.
    - Si un pare-feu importé utilise une politique de pare-feu associée à un pare-feu qui ne fait pas partie de l'ensemble de ressources de la stratégie. Cela peut se produire parce qu'un pare-feu peut avoir exactement une politique de pare-feu, mais une seule politique de pare-feu peut être associée à plusieurs pare-feux.
    - Si un groupe de règles préexistant appartenant à la politique de pare-feu d'un pare-feu importé qui est également spécifiée dans la stratégie Firewall Manager reçoit une priorité différente.
  - Si vous activez le nettoyage des ressources dans la politique, Firewall Manager supprime les groupes de règles qui figuraient dans la politique d'importation FMS des pare-feux concernés par le jeu de ressources.
  - Les pare-feux gérés par ceux gérés par une importation de Firewall Manager. Le type de gestion de pare-feu existant ne peut être géré que par une seule politique à la fois. Si le même ensemble de ressources est ajouté à plusieurs politiques de pare-feu du réseau d'importation, les pare-feux du jeu de ressources seront gérés par la première stratégie à laquelle le jeu de ressources a été ajouté et seront ignorés par la seconde stratégie.

- Firewall Manager ne diffuse actuellement pas les configurations de politique d'exception. Pour plus d'informations sur les politiques d'exception relatives aux flux, consultez la section Politique d'exception aux flux dans le Guide du AWS Network Firewall développeur.

Si vous modifiez la liste des zones de disponibilité pour les politiques utilisant une gestion de pare-feu distribuée ou centralisée, Firewall Manager essaiera de nettoyer tous les points de terminaison créés dans le passé, mais qui ne sont pas actuellement concernés par la politique. Firewall Manager supprimera le point de terminaison uniquement s'il n'existe aucune route de table de routage faisant référence au point de terminaison hors de portée. Si Firewall Manager s'aperçoit qu'il n'est pas en mesure de supprimer ces points de terminaison, il marquera le sous-réseau du pare-feu comme étant non conforme et continuera à essayer de supprimer le point de terminaison jusqu'à ce qu'il soit possible de le supprimer en toute sécurité.

Comment Firewall Manager gère vos sous-réseaux de pare-feu

Les sous-réseaux de pare-feu sont les sous-réseaux VPC créés par Firewall Manager pour les points de terminaison du pare-feu qui filtrent le trafic réseau. Chaque point de terminaison du pare-feu doit être déployé dans un sous-réseau VPC dédié. Firewall Manager crée au moins un sous-réseau de pare-feu dans chaque VPC concerné par la politique.

Pour les politiques qui utilisent le modèle de déploiement distribué avec configuration automatique des points de terminaison, Firewall Manager crée uniquement des sous-réseaux de pare-feu dans les zones de disponibilité qui possèdent un sous-réseau avec une route de passerelle Internet ou un sous-réseau avec une route vers les points de terminaison du pare-feu créés par Firewall Manager pour sa politique. Pour plus d'informations, consultez VPC et sous-réseaux dans le Guide de l'utilisateur Amazon VPC.

Pour les politiques qui utilisent le modèle distribué ou centralisé dans lequel vous spécifiez les zones de disponibilité dans lesquelles Firewall Manager crée les points de terminaison du pare-feu, Firewall Manager crée un point de terminaison dans ces zones de disponibilité spécifiques, qu'il existe ou non d'autres ressources dans la zone de disponibilité.

Lorsque vous définissez pour la première fois une politique de Network Firewall, vous spécifiez la manière dont Firewall Manager gère les sous-réseaux de pare-feu dans chacun des VPC concernés. Vous ne pourrez pas modifier ce choix ultérieurement.

Pour les politiques qui utilisent le modèle de déploiement distribué avec configuration automatique des points de terminaison, vous pouvez choisir entre les options suivantes :

- Déployez un sous-réseau de pare-feu pour chaque zone de disponibilité dotée de sous-réseaux publics. Il s'agit du comportement de par défaut. Cela garantit une haute disponibilité de vos protections de filtrage du trafic.
- Déployez un sous-réseau de pare-feu unique dans une zone de disponibilité. Avec ce choix, Firewall Manager identifie la zone du VPC qui possède le plus grand nombre de sous-réseaux publics et y crée le sous-réseau de pare-feu. Le point de terminaison unique du pare-feu filtre tout le trafic réseau pour le VPC. Cela peut réduire les coûts du pare-feu, mais il n'est pas hautement disponible et nécessite que le trafic en provenance d'autres zones franchisse les limites des zones pour être filtré.

Pour les politiques qui utilisent le modèle de déploiement distribué avec une configuration de point de terminaison personnalisée ou le modèle de déploiement centralisé, Firewall Manager crée les sous-réseaux dans les zones de disponibilité spécifiées qui entrent dans le champ d'application de la politique.

Vous pouvez fournir des blocs d'adresse CIDR VPC que Firewall Manager utilisera pour les sous-réseaux du pare-feu ou vous pouvez laisser à Firewall Manager le choix des adresses de point de terminaison du pare-feu.

- Si vous ne fournissez pas de blocs CIDR, Firewall Manager interroge vos VPC pour connaître les adresses IP disponibles à utiliser.
- Si vous fournissez une liste de blocs d'adresse CIDR, Firewall Manager recherche de nouveaux sous-réseaux uniquement dans les blocs d'adresse CIDR que vous fournissez. Vous devez utiliser des blocs d'adresse CIDR /28. Pour chaque sous-réseau de pare-feu créé, Firewall Manager parcourt votre liste de blocs CIDR et utilise le premier qu'il trouve applicable à la zone de disponibilité et au VPC et dont les adresses sont disponibles. Si Firewall Manager ne trouve pas d'espace libre dans le VPC (avec ou sans restriction), le service ne créera pas de pare-feu dans le VPC.

Si Firewall Manager ne parvient pas à créer le sous-réseau de pare-feu requis dans une zone de disponibilité, il marque le sous-réseau comme non conforme à la politique. Lorsque la zone est dans cet état, le trafic de la zone doit franchir les limites de la zone pour être filtré par un point de terminaison situé dans une autre zone. Ce scénario est similaire au scénario d'un sous-réseau de pare-feu unique.

Comment Firewall Manager gère les ressources de votre Network Firewall

Lorsque vous définissez la politique dans Firewall Manager, vous fournissez le comportement de filtrage du trafic réseau d'une politique de AWS Network Firewall pare-feu standard. Vous ajoutez des groupes de règles de Network Firewall apatrides et statiques et vous spécifiez des actions par défaut pour les paquets qui ne correspondent à aucune règle apatride. Pour plus d'informations sur l'utilisation des politiques de pare-feu dans AWS Network Firewall, consultez les politiques de AWS Network Firewall pare-feu.

Pour les politiques distribuées et centralisées, lorsque vous enregistrez la politique Network Firewall, Firewall Manager crée un pare-feu et une politique de pare-feu dans chaque VPC concerné par cette politique. Firewall Manager nomme ces ressources Network Firewall en concaténant les valeurs suivantes :

- Chaîne fixe, soit, `FMManagedNetworkFirewall` soit`FMManagedNetworkFirewallPolicy`, selon le type de ressource.
- Nom de la politique de Firewall Manager. Il s'agit du nom que vous attribuez lorsque vous créez la politique.
- ID de politique Firewall Manager. Il s'agit de l'ID de AWS ressource pour la politique Firewall Manager.
- ID Amazon VPC. Il s'agit de l'ID de AWS ressource du VPC dans lequel Firewall Manager crée le pare-feu et la politique de pare-feu.

Voici un exemple de nom pour un pare-feu géré par Firewall Manager :

```
FMManagedNetworkFirewallEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Voici un exemple de nom de politique de pare-feu :

```
FMManagedNetworkFirewallPolicyEXAMPLENameEXAMPLEFirewallManagerPolicyIdEXAMPLEVPCId
```

Une fois que vous avez créé la politique, les comptes membres des VPC ne peuvent pas remplacer vos paramètres de politique de pare-feu ou vos groupes de règles, mais ils peuvent ajouter des groupes de règles à la politique de pare-feu créée par Firewall Manager.

Comment Firewall Manager gère et surveille les tables de routage VPC conformément à votre politique

> **Note**
>
> La gestion des tables de routage n'est actuellement pas prise en charge pour les politiques qui utilisent le modèle de déploiement centralisé.

Lorsque Firewall Manager crée les points de terminaison de votre pare-feu, il crée également les tables de routage VPC correspondantes. Firewall Manager ne gère toutefois pas vos tables de routage VPC. Vous devez configurer les tables de routage de votre VPC pour diriger le trafic réseau vers les points de terminaison du pare-feu créés par Firewall Manager. À l'aide des améliorations apportées au routage d'entrée d'Amazon VPC, modifiez vos tables de routage pour acheminer le trafic via les nouveaux points de terminaison du pare-feu. Vos modifications doivent insérer les points de terminaison du pare-feu entre les sous-réseaux que vous souhaitez protéger et les emplacements extérieurs. Le routage exact que vous devez effectuer dépend de votre architecture et de ses composants.

Firewall Manager permet actuellement de surveiller les itinéraires de votre table de routage VPC pour détecter tout trafic destiné à la passerelle Internet qui contourne le pare-feu. Firewall Manager ne prend pas en charge les autres passerelles cibles telles que les passerelles NAT.

Pour plus d'informations sur la gestion des tables de routage pour votre VPC, consultez la section Gestion des tables de routage pour votre VPC dans le guide de l'utilisateur Amazon Virtual Private Cloud. Pour plus d'informations sur la gestion de vos tables de routage pour Network Firewall, consultez la section Configurations des tables de routage AWS Network Firewall dans le manuel du AWS Network Firewall développeur.

Lorsque vous activez la surveillance d'une politique, Firewall Manager surveille en permanence les configurations de routage du VPC et vous alerte en cas de trafic qui contourne l'inspection du pare-feu pour ce VPC. Si un sous-réseau possède une route de point de terminaison de pare-feu, Firewall Manager recherche les routes suivantes :

- Itinéraires pour envoyer le trafic vers le point de terminaison Network Firewall.
- Itinéraires permettant de transférer le trafic du point de terminaison Network Firewall vers la passerelle Internet.
- Routes entrantes entre la passerelle Internet et le point de terminaison Network Firewall.
- Routes depuis le sous-réseau du pare-feu.

Si un sous-réseau possède un itinéraire Network Firewall mais que le routage est asymétrique dans Network Firewall et dans la table de routage de votre passerelle Internet, Firewall Manager signale le sous-réseau comme non conforme. Firewall Manager détecte également les itinéraires vers la passerelle Internet dans la table de routage du pare-feu créée par Firewall Manager, ainsi que dans la table de routage de votre sous-réseau, et les signale comme non conformes. Les routes supplémentaires figurant dans la table de routage du sous-réseau Network Firewall et dans la table de routage de votre passerelle Internet sont également signalées comme non conformes. En fonction du type de violation, Firewall Manager suggère des mesures correctives pour mettre en conformité la configuration de l'itinéraire. Firewall Manager ne propose pas de suggestions dans tous les cas. Par exemple, si le sous-réseau de votre client possède un point de terminaison de pare-feu créé en dehors de Firewall Manager, Firewall Manager ne suggère aucune action corrective.

Par défaut, Firewall Manager marquera comme non conforme tout trafic franchissant les limites de la zone de disponibilité pour inspection. Toutefois, si vous choisissez de créer automatiquement un point de terminaison unique dans votre VPC, Firewall Manager ne marquera pas le trafic franchissant la limite de la zone de disponibilité comme non conforme.

Pour les politiques qui utilisent des modèles de déploiement distribués avec une configuration de point de terminaison personnalisée, vous pouvez choisir si le trafic traversant la limite de la zone de disponibilité depuis une zone de disponibilité sans point de terminaison de pare-feu est marqué comme conforme ou non conforme.

> **Note**
>
> - Firewall Manager ne suggère aucune action corrective pour les routes non IPv4, telles que IPv6 et les routes de liste de préfixes.
> - La détection des appels effectués à l'aide de l'appel d'`DisassociateRouteTable`API peut prendre jusqu'à 12 heures.
> - Firewall Manager crée une table de routage Network Firewall pour un sous-réseau qui contient les points de terminaison du pare-feu. Firewall Manager part du principe que cette table de routage contient uniquement des passerelles Internet et des routes par défaut VPC valides. Toute route supplémentaire ou non valide dans cette table de routage est considérée comme non conforme.

Lorsque vous configurez votre politique de Firewall Manager, si vous choisissez le mode Monitor, Firewall Manager fournit des informations sur les violations de ressources et les mesures correctives

concernant vos ressources. Vous pouvez utiliser ces actions correctives suggérées pour résoudre les problèmes de routage dans vos tables de routage. Si vous choisissez le mode Off, Firewall Manager ne surveille pas le contenu de votre table de routage à votre place. Avec cette option, vous gérez vous-même vos tables de routage VPC. Pour plus d'informations sur ces violations des ressources, consultezAfficher les informations de conformité d'une AWS Firewall Manager politique.

> **Warning**
>
> Si vous choisissez Monitor dans le cadre de la configuration des AWS Network Firewall itinéraires lors de la création de votre politique, vous ne pouvez pas le désactiver pour cette stratégie. Toutefois, si vous choisissez Désactivé, vous pourrez l'activer ultérieurement.

Configuration de la journalisation pour une AWS Network Firewall politique

Vous pouvez activer la journalisation centralisée pour vos politiques de Network Firewall afin d'obtenir des informations détaillées sur le trafic au sein de votre organisation. Vous pouvez sélectionner la journalisation des flux pour capturer le flux du trafic réseau, ou la journalisation des alertes pour signaler le trafic correspondant à une règle dont l'action de règle est définie sur `DROP` ou`ALERT`. Pour plus d'informations sur la AWS Network Firewall journalisation, consultez la section Enregistrement du trafic réseau depuis AWS Network Firewall le Guide du AWS Network Firewall développeur.

Vous envoyez des journaux depuis les pare-feux Network Firewall de votre politique vers un compartiment Amazon S3. Une fois que vous avez activé la journalisation, AWS Network Firewall fournit les journaux pour chaque Network Firewall configuré en mettant à jour les paramètres du pare-feu afin de transmettre les journaux aux compartiments Amazon S3 que vous avez sélectionnés avec le AWS Firewall Manager préfixe réservé,. `<policy-name>-<policy-id>`

> **Note**
>
> Ce préfixe est utilisé par Firewall Manager pour déterminer si une configuration de journalisation a été ajoutée par Firewall Manager ou si elle a été ajoutée par le propriétaire du compte. Si le propriétaire du compte tente d'utiliser le préfixe réservé pour sa propre journalisation personnalisée, il est remplacé par la configuration de journalisation définie dans la politique de Firewall Manager.

Pour plus d'informations sur la façon de créer un compartiment Amazon S3 et de consulter les journaux stockés, consultez Qu'est-ce qu'Amazon S3 ? dans le guide de l'utilisateur d'Amazon Simple Storage Service.

Pour activer la journalisation, vous devez satisfaire aux exigences suivantes :

- L'Amazon S3 que vous spécifiez dans votre politique Firewall Manager doit exister.
- Vous devez détenir les autorisations suivants :
  - `logs:CreateLogDelivery`
  - `s3:GetBucketPolicy`
  - `s3:PutBucketPolicy`
- Si le compartiment Amazon S3 qui est votre destination de journalisation utilise un chiffrement côté serveur avec des clés qui y sont stockées AWS Key Management Service, vous devez ajouter la politique suivante à votre clé AWS KMS gérée par le client afin de permettre à Firewall Manager de se connecter à votre CloudWatch groupe de journaux Logs :

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": "delivery.logs.amazonaws.com"
    },
    "Action": [
        "kms:Encrypt*",
        "kms:Decrypt*",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:Describe*"
    ],
    "Resource": "*"
}
```

Notez que seuls les buckets du compte administrateur de Firewall Manager peuvent être utilisés pour la journalisation AWS Network Firewall centralisée.

Lorsque vous activez la connexion centralisée dans le cadre d'une politique de Network Firewall, Firewall Manager effectue les actions suivantes sur votre compte :

- Firewall Manager met à jour les autorisations sur les compartiments S3 sélectionnés pour permettre la livraison des journaux.
- Firewall Manager crée des répertoires dans le compartiment S3 pour chaque compte membre dans le cadre de la politique. Les journaux de chaque compte se trouvent à l'adresse`<bucket-name>/<policy-name>-<policy-id>/AWSLogs/<account-id>`.

Pour activer la journalisation dans le cadre d'une politique Network Firewall

1. Créez un compartiment Amazon S3 à l'aide de votre compte administrateur Firewall Manager. Pour plus d'informations, consultez la section Création d'un compartiment dans le guide de l'utilisateur d'Amazon Simple Storage Service.
2. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

3. Dans le volet de navigation, sélectionnez Security Policies.
4. Choisissez la politique Network Firewall pour laquelle vous souhaitez activer la journalisation. Pour plus d'informations sur la AWS Network Firewall journalisation, consultez la section Enregistrement du trafic réseau depuis AWS Network Firewall le Guide du AWS Network Firewall développeur.
5. Dans l'onglet Détails de la politique, dans la section Règles de politique, choisissez Modifier.
6. Pour activer et agréger les journaux, choisissez une ou plusieurs options dans Configuration de la journalisation :
   - Activer et agréger les journaux de flux
   - Activer et agréger les journaux d'alertes
7. Choisissez le compartiment Amazon S3 dans lequel vous souhaitez que vos journaux soient livrés. Vous devez choisir un compartiment pour chaque type de journal que vous activez. Vous pouvez utiliser le même compartiment pour les deux types de journaux.

8. (Facultatif) Si vous souhaitez que la journalisation personnalisée créée par le compte membre soit remplacée par la configuration de journalisation définie dans la politique, choisissez Remplacer la configuration de journalisation existante.
9. Choisissez Suivant.
10. Vérifiez vos paramètres, puis choisissez Enregistrer pour enregistrer les modifications apportées à la politique.

Pour désactiver la journalisation dans le cadre d'une politique Network Firewall

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Security Policies.
3. Choisissez la politique Network Firewall pour laquelle vous souhaitez désactiver la journalisation.
4. Dans l'onglet Détails de la politique, dans la section Règles de politique, choisissez Modifier.
5. Sous État de la configuration de la journalisation, désélectionnez Activer et agréger les journaux de flux et Activer et agréger les journaux d'alertes s'ils sont sélectionnés.
6. Choisissez Suivant.
7. Vérifiez vos paramètres, puis choisissez Enregistrer pour enregistrer les modifications apportées à la politique.

Politiques de pare-feu DNS d'Amazon Route 53 Resolver

Vous pouvez utiliser les politiques de pare-feu AWS Firewall Manager DNS pour gérer les associations entre les groupes de règles du pare-feu DNS Amazon Route 53 Resolver et vos VPC Amazon Virtual Private Cloud au sein de votre organisation dans. AWS Organizations Vous pouvez appliquer des groupes de règles contrôlés de manière centralisée à l'ensemble de votre organisation ou à un sous-ensemble sélectionné de vos comptes et VPC.

Le pare-feu DNS permet de filtrer et de réguler le trafic DNS sortant pour vos VPC. Vous créez des ensembles réutilisables de règles de filtrage dans les groupes de règles du pare-feu DNS et vous associez les groupes de règles à vos VPC. Lorsque vous appliquez la politique Firewall Manager, pour chaque compte et VPC relevant du champ d'application de la stratégie, Firewall Manager crée une association entre chaque groupe de règles de pare-feu DNS de la stratégie et chaque VPC inclus dans le champ d'application de la stratégie, en utilisant les paramètres de priorité d'association que vous spécifiez dans la politique de Firewall Manager.

Pour plus d'informations sur l'utilisation du pare-feu DNS, consultez le pare-feu DNS Amazon Route 53 Resolver dans le guide du développeur Amazon Route 53.

Les sections suivantes décrivent les exigences relatives à l'utilisation des politiques de pare-feu DNS de Firewall Manager et décrivent le fonctionnement de ces politiques. Pour la procédure de création de la politique, voirCréation d'une AWS Firewall Manager politique pour le pare-feu DNS Amazon Route 53 Resolver.

Vous devez activer le partage des ressources

Une politique de pare-feu DNS partage les groupes de règles de pare-feu DNS entre les comptes de votre organisation. Pour que cela fonctionne, le partage des ressources doit être activé avec AWS Organizations. Pour plus d'informations sur la façon d'activer le partage des ressources, consultezPartage des ressources pour les politiques de Network Firewall et de DNS Firewall.

Les groupes de règles de votre pare-feu DNS doivent être définis

Lorsque vous spécifiez une nouvelle politique de pare-feu DNS, vous définissez les groupes de règles de la même manière que lorsque vous utilisez directement le pare-feu DNS d'Amazon Route 53 Resolver. Vos groupes de règles doivent déjà exister dans le compte administrateur de Firewall Manager pour que vous puissiez les inclure dans la politique. Pour plus d'informations sur la création de groupes de règles de pare-feu DNS, consultez la section Groupes de règles et règles de pare-feu DNS.

Vous définissez les associations de groupes de règles les plus basses et les plus prioritaires

Les associations de groupes de règles de pare-feu DNS que vous gérez via les politiques de pare-feu DNS de Firewall Manager contiennent les associations les moins prioritaires et les associations les plus prioritaires pour vos VPC. Dans la configuration de votre politique, ils apparaissent en tant que premier et dernier groupe de règles.

Le pare-feu DNS filtre le trafic DNS pour le VPC dans l'ordre suivant :

1. Premiers groupes de règles, définis par vos soins dans la politique de pare-feu DNS de Firewall Manager. Les valeurs valides sont comprises entre 1 et 99.
2. Groupes de règles de pare-feu DNS associés par des gestionnaires de comptes individuels via le pare-feu DNS.
3. Derniers groupes de règles, que vous avez définis dans la politique de pare-feu DNS de Firewall Manager. Les valeurs valides sont comprises entre 9 901 et 10 000.

Suppression d'un groupe de règles

Pour supprimer un groupe de règles d'une politique de pare-feu DNS de Firewall Manager, vous devez effectuer les étapes suivantes :

1. Supprimez le groupe de règles de votre politique de pare-feu DNS Firewall Manager.
2. Annulation du partage du groupe de règles dans. AWS Resource Access Manager Pour annuler le partage d'un groupe de règles dont vous êtes propriétaire, vous devez le supprimer du partage de ressources. Vous pouvez le faire à l'aide de la AWS RAM console ou de la AWS CLI. Pour plus d'informations sur l'annulation du partage d'une ressource, voir Mettre à jour un partage de ressources AWS RAM dans le Guide de l'AWS RAM utilisateur.
3. Supprimez le groupe de règles à l'aide de la console ou de la AWS CLI du pare-feu DNS.

Comment Firewall Manager nomme les associations de groupes de règles qu'il crée

Lorsque vous enregistrez la politique de pare-feu DNS, si vous avez activé la correction automatique, Firewall Manager crée une association de pare-feu DNS entre les groupes de règles que vous avez fournis dans la stratégie et les VPC concernés par la stratégie. Firewall Manager nomme ces associations en concaténant les valeurs suivantes :

- La chaîne fixe,`FMManaged_`.
- L'ID de politique de Firewall Manager. Il s'agit de l'ID de AWS ressource pour la politique Firewall Manager.

Voici un exemple de nom pour un pare-feu géré par Firewall Manager :

```
FMManaged_EXAMPLEDNSFirewallPolicyId
```

Après avoir créé la politique, si les propriétaires de comptes dans les VPC remplacent les paramètres de votre politique de pare-feu ou vos associations de groupes de règles, Firewall Manager marquera la politique comme non conforme et essaiera de proposer une action corrective. Les propriétaires de comptes peuvent associer d'autres groupes de règles de pare-feu DNS aux VPC concernés par la politique de pare-feu DNS. Toutes les associations créées par les propriétaires de comptes individuels doivent disposer de paramètres de priorité entre la première et la dernière association de groupes de règles.

Politiques NGFW de Palo Alto Networks Cloud

Le pare-feu cloud de nouvelle génération (NGFW) de Palo Alto Networks est un service de pare-feu tiers que vous pouvez utiliser pour vos politiques. AWS Firewall Manager Avec Palo Alto Networks Cloud NGFW for Firewall Manager, vous pouvez créer et déployer de manière centralisée des ressources et des ensembles de règles Palo Alto Networks Cloud NGFW sur tous vos comptes. AWS

Pour utiliser Palo Alto Networks Cloud NGFW avec Firewall Manager, vous devez d'abord vous abonner au service Pay-As-You-Go de Palo Alto Networks Cloud NGFW sur le Marketplace. AWS Après votre inscription, vous effectuez une série d'étapes dans le service Cloud NGFW de Palo Alto Networks pour configurer votre compte et les paramètres Cloud NGFW. Ensuite, vous créez une politique Firewall Manager Cloud FMS pour déployer et gérer de manière centralisée les ressources et les règles du Cloud NGFW de Palo Alto Networks sur tous les comptes de vos Organizations. AWS

Pour la procédure de création de la politique de Firewall Manager, consultezCréation d'une AWS Firewall Manager politique pour Palo Alto Networks Cloud NGFW. Pour plus d'informations sur la configuration et la gestion de Palo Alto Networks Cloud NGFW pour Firewall Manager, consultez le Palo Alto Networks Cloud NGFW de Palo Alto Networks dans la documentation. AWS

Politiques de pare-feu natif du cloud (CNF) de Fortigate en tant que service

Fortigate Cloud Native Firewall (CNF) as a Service est un service de pare-feu tiers que vous pouvez utiliser pour vos politiques. AWS Firewall Manager Fortigate CNF est un service de pare-feu de nouvelle génération qui vous permet de protéger facilement vos réseaux cloud et de gérer vos politiques de sécurité. Avec Fortigate CNF for Firewall Manager, vous pouvez créer et déployer de manière centralisée des ressources et des ensembles de politiques Fortigate CNF sur tous vos comptes. AWS

Pour utiliser Fortigate CNF avec Firewall Manager, vous devez d'abord vous abonner au Fortigate Cloud Native Firewall (CNF) en tant que service sur le Marketplace. AWS Après votre inscription,

vous effectuez une série d'étapes dans le service Fortigate CNF pour configurer vos ensembles de politiques globaux et d'autres paramètres. Ensuite, vous créez une politique Firewall Manager pour déployer et gérer de manière centralisée les ressources Fortigate CNF sur tous les comptes de vos Organizations. AWS

Pour la procédure de création d'une politique Fortigate CNF Firewall Manager, consultez. Création d'une AWS Firewall Manager politique pour Fortigate Cloud Native Firewall (CNF) en tant que service Pour plus d'informations sur la configuration et la gestion de Fortigate CNF pour une utilisation avec Firewall Manager, consultez la documentation de Fortigate CNF.

Partage des ressources pour les politiques de Network Firewall et de DNS Firewall

Pour gérer les politiques de Firewall Manager Network Firewall et de DNS Firewall, vous devez activer le partage des ressources avec AWS Organizations in AWS Resource Access Manager. Cela permet à Firewall Manager de déployer des protections sur l'ensemble de vos comptes lorsque vous créez ces types de politiques.

Pour activer le partage des ressources, suivez les instructions de la section Activer le partage avec AWS Organizations dans le guide de AWS Resource Access Manager l'utilisateur.

Problèmes liés au partage des ressources

Vous pouvez rencontrer des problèmes avec le partage des ressources, soit lorsque vous l' AWS RAM activez, soit lorsque vous travaillez sur des politiques de Firewall Manager qui l'exigent.

Voici quelques exemples de ces problèmes :

- Lorsque vous suivez les instructions pour activer le partage, dans la AWS RAM console, le choix Activer le partage avec AWS Organizations est grisé et n'est pas disponible pour la sélection.
- Lorsque vous travaillez dans Firewall Manager sur une politique qui nécessite le partage des ressources, celle-ci est marquée comme non conforme et des messages s'affichent indiquant que le partage des ressources est activé AWS RAM ou non.

Si vous rencontrez des problèmes avec le partage des ressources, suivez la procédure ci-dessous pour essayer de l'activer.

Réessayez d'activer le partage des ressources

- Réessayez d'activer le partage à l'aide de l'une des options suivantes :

- (Option) Dans la AWS RAM console, suivez les instructions de la section Activer le partage avec AWS Organizations dans le guide de AWS Resource Access Manager l'utilisateur.
- (Option) À l'aide de l' AWS RAM API, appelez`EnableSharingWithAwsOrganization`. Consultez la documentation à l'adresse EnableSharingWithAwsOrganization.

Utilisation des ensembles de ressources dans Firewall Manager

Un ensemble de AWS Firewall Manager ressources est un ensemble de ressources, telles que des pare-feux, que vous pouvez regrouper et gérer dans le cadre d'une politique Firewall Manager. Les ensembles de ressources permettent aux membres de votre organisation d'avoir un contrôle précis sur les ressources à gérer dans le cadre d'une politique. Pour utiliser des ensembles de ressources, créez un ensemble de ressources dans la console ou à l'aide de l'PutResourceSetAPI, puis ajoutez-le à votre politique Firewall Manager.

Vous pouvez créer et gérer des ensembles de ressources pour les types de ressources et de politiques de sécurité suivants :

Type de ressource	Type de politique de sécurité Firewall Manager
AWS Network Firewall - pare-feux	Politique de Network Firewall : utilisez des ensembles de ressources pour importer des pare-feux existants depuis Network Firewall. Pour plus d'informations sur l'utilisation des ensembles de ressources dans une politique Network Firewall, consultez l'étape Importation de pare-feux existants de la Création d'une AWS Firewall Manager politique pour AWS Network Firewall procédure.

Les sections suivantes décrivent les exigences relatives à la création et à la suppression d'ensembles de ressources.

Rubriques

- Considérations relatives à l'utilisation d'ensembles de ressources dans Firewall Manager
- Création d'ensembles de ressources
- Supprimer un ensemble de ressources

Considérations relatives à l'utilisation d'ensembles de ressources dans Firewall Manager

Tenez compte des considérations suivantes lorsque vous travaillez avec des ensembles de ressources

Références à des ressources inexistantes

Lorsque vous ajoutez une ressource à un ensemble de ressources, vous créez une référence à la ressource à l'aide d'un Amazon Resource Name (ARN). Firewall Manager vérifie que le format Amazon Resource Name (ARN) est correct, mais Firewall Manager ne vérifie pas l'existence de la ressource référencée. Si la ressource n'existe pas encore passe la validation ARN, Firewall Manager inclut la référence de ressource dans le jeu de ressources. Si une nouvelle ressource avec le même ARN est créée ultérieurement, Firewall Manager applique à la nouvelle ressource des groupes de règles issus de la politique associée à l'ensemble de ressources.

Ressources supprimées

Lorsqu'une ressource d'un ensemble de ressources est supprimée, la référence à la ressource reste dans le jeu de ressources jusqu'à ce qu'elle soit supprimée par l'administrateur de Firewall Manager.

Ressources détenues par le compte d'un membre qui quitte l' AWS Organizations organisation

Si un compte membre quitte l'organisation, toutes les références aux ressources détenues par ce compte membre resteront dans l'ensemble de ressources mais ne seront plus gérées par les politiques auxquelles l'ensemble de ressources est associé.

Association à plusieurs politiques

Un ensemble de ressources peut être associé à plusieurs politiques, mais tous les types de politiques ne prennent pas en charge plusieurs politiques gérant la même ressource. Consultez la documentation de votre type de politique spécifique pour obtenir des informations sur les scénarios non pris en charge.

Création d'ensembles de ressources

Pour créer un ensemble de ressources (console)

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/

wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

> **Note**
>
> Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Resource sets.
3. Choisissez Créer un ensemble de ressources.
4. Pour Nom du jeu de ressources, entrez un nom descriptif.
5. (Facultatif) entrez une description pour l'ensemble de ressources.
6. Choisissez Suivant.
7. Pour Choisir les ressources, sélectionnez un ID de AWS compte, puis sélectionnez Choisir les ressources pour ajouter les ressources détenues et gérées par ce compte à l'ensemble de ressources. Après avoir sélectionné les ressources, sélectionnez Ajouter pour ajouter les ressources à l'ensemble de ressources.
8. Choisissez Suivant.
9. Pour les balises d'ensemble de ressources, ajoutez les balises d'identification que vous souhaitez pour l'ensemble de ressources. Pour plus d'informations sur les balises, consultez Utilisation de Tag Editor.
10. Choisissez Suivant.
11. Passez en revue le nouvel ensemble de ressources. Pour apporter des modifications, choisissez Modifier dans la zone que vous souhaitez modifier. Cela vous ramène à l'étape correspondante de l'assistant de création. Lorsque vous êtes satisfait de l'ensemble de ressources, choisissez Créer un ensemble de ressources.

Supprimer un ensemble de ressources

Avant de pouvoir supprimer un ensemble de ressources, celui-ci doit être dissocié de toutes les politiques utilisant le jeu de ressources. Vous pouvez dissocier les groupes de ressources sur la page détaillée de la politique à l'aide de la console ou de l'PutPolicyAPI.

Pour supprimer un ensemble de ressources (console)

1. Dans le volet de navigation, sélectionnez Resource sets.

2. Choisissez l'option située à côté de l'ensemble de ressources que vous souhaitez supprimer.
3. Sélectionnez Supprimer.

Afficher les informations de conformité d'une AWS Firewall Manager politique

Cette section fournit des conseils pour visualiser l'état de conformité des comptes et des ressources concernés par une AWS Firewall Manager politique. Pour plus d'informations sur les contrôles mis en place AWS pour garantir la sécurité et la conformité du cloud, consultezValidation de conformité pour Firewall Manager.

> **Note**
>
> Pour que Firewall Manager puisse contrôler le respect des politiques, AWS Config il doit enregistrer en permanence les modifications de configuration des ressources protégées. Dans votre AWS Config configuration, la fréquence d'enregistrement doit être réglée sur Continuous, qui est le réglage par défaut.

> **Note**
>
> Pour maintenir un état de conformité correct dans vos ressources protégées, évitez de modifier à plusieurs reprises l'état des protections Firewall Manager, automatiquement ou manuellement. Firewall Manager utilise les informations provenant de AWS Config pour détecter les modifications apportées aux configurations des ressources. Si les modifications sont appliquées assez rapidement, AWS Config vous risquez de perdre la trace de certaines d'entre elles, ce qui peut entraîner la perte d'informations sur la conformité ou l'état des mesures correctives dans Firewall Manager.
> Si vous constatez qu'une ressource que vous protégez avec Firewall Manager présente un statut de conformité ou de correction incorrect, assurez-vous d'abord que vous n'exécutez aucun processus qui modifie ou réinitialise vos protections Firewall Manager, puis actualisez le AWS Config suivi de la ressource en réévaluant les règles de configuration associées dans. AWS Config

Pour toutes les AWS Firewall Manager politiques, vous pouvez consulter l'état de conformité des comptes et des ressources concernés par la politique. Un compte ou une ressource est conforme à une politique de Firewall Manager si les paramètres de cette politique sont reflétés dans les paramètres du compte ou de la ressource. Chaque type de politique a ses propres exigences de conformité, que vous pouvez ajuster lorsque vous définissez la stratégie. Pour certaines politiques, vous pouvez également consulter des informations détaillées sur les violations pour les ressources concernées, afin de mieux comprendre et gérer les risques de sécurité.

Pour consulter les informations de conformité d'une politique

1. Connectez-vous à l' AWS Management Console aide de votre compte administrateur Firewall Manager, puis ouvrez la console Firewall Manager à l'adressehttps://console.aws.amazon.com/wafv2/fmsv2. Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

   > **Note**
   >
   > Pour plus d'informations sur la configuration d'un compte administrateur Firewall Manager, consultez AWS Firewall Manager prérequis.

2. Dans le volet de navigation, sélectionnez Stratégies de sécurité.
3. Choisissez une stratégie. Dans l'onglet Comptes et ressources de la page de politique, Firewall Manager répertorie les comptes de votre organisation, regroupés en fonction de ceux qui entrent dans le champ d'application de la politique et de ceux qui ne le sont pas.

   Le volet Accounts within policy scope répertorie le statut de conformité de chaque compte. Un statut Conforme indique que la politique a été appliquée avec succès à toutes les ressources incluses dans le champ d'application du compte. Un statut Non conforme indique que la politique n'a pas été appliquée à une ou plusieurs des ressources concernées par le compte.
4. Choisissez un compte non conforme. Sur la page du compte, Firewall Manager répertorie l'ID et le type de chaque ressource non conforme ainsi que la raison pour laquelle la ressource enfreint la politique.

   > **Note**
   >
   > Pour les types de ressources `AWS::EC2::NetworkInterface` (ENI) et`AWS::EC2::Instance`, Firewall Manager peut afficher un nombre limité de

ressources non conformes. Pour répertorier d'autres ressources non conformes, corrigez celles qui sont initialement affichées pour le compte.

5. Si le type de stratégie Firewall Manager est une stratégie de groupe de sécurité d'audit de contenu, vous pouvez accéder aux informations détaillées sur les violations relatives à une ressource.

   Pour afficher les détails de la violation, choisissez la ressource.

   > **Note**
   >
   > Les ressources que Firewall Manager a jugées non conformes avant l'ajout de la page détaillée sur les violations de ressources ne contiennent peut-être pas de détails sur les violations.

   Sur la page des ressources, Firewall Manager répertorie les détails spécifiques de la violation, en fonction du type de ressource.

   - **`AWS::EC2::NetworkInterface`**(ENI) — Firewall Manager affiche des informations sur le groupe de sécurité auquel la ressource n'est pas conforme. Choisissez le groupe de sécurité pour en savoir plus.
   - **`AWS::EC2::Instance`**— Firewall Manager affiche l'ENI attachée à l'instance EC2 non conforme. Il affiche également des informations sur le groupe de sécurité auquel les ressources ne sont pas conformes. Choisissez le groupe de sécurité pour en savoir plus.
   - **`AWS::EC2::SecurityGroup`**— Firewall Manager affiche les informations relatives aux violations suivantes :
     - Règle de groupe de sécurité non conforme : règle en violation, y compris son protocole, sa plage de ports, sa plage d'adresses IP CIDR et sa description.
     - Règle référencée : règle du groupe de sécurité d'audit violée par la règle du groupe de sécurité non conforme, avec ses détails.
     - Motifs de violation — Explication de la constatation de non-conformité.
     - Action corrective — Mesures suggérées à prendre. Si Firewall Manager ne parvient pas à déterminer une action corrective sûre, ce champ est vide.
   - **`AWS::EC2::Subnet`**— Ceci est utilisé pour les politiques d'ACL réseau et de Network Firewall.

Firewall Manager affiche l'ID du sous-réseau, l'ID du VPC et la zone de disponibilité. Le cas échéant, Firewall Manager inclut des informations supplémentaires sur la violation. Le composant de description de la violation contient une description de l'état attendu de la ressource, de l'état actuel non conforme et, le cas échéant, une description de la cause de l'écart.

Violations du Network Firewall

- Violations de gestion des itinéraires : pour les politiques de Network Firewall qui utilisent le mode Monitor, Firewall Manager affiche des informations de base sur le sous-réseau, ainsi que les itinéraires attendus et réels dans le sous-réseau, la passerelle Internet et la table de routage du sous-réseau Network Firewall. Firewall Manager vous alerte en cas de violation si les itinéraires réels ne correspondent pas aux itinéraires attendus dans la table de routage.
- Actions de correction pour les violations de gestion des itinéraires : pour les politiques de Network Firewall qui utilisent le mode Monitor, Firewall Manager suggère des actions correctives possibles sur les configurations de route présentant des violations.

Par exemple, supposons qu'un sous-réseau est censé envoyer du trafic via les points de terminaison du pare-feu, mais que le sous-réseau actuel envoie le trafic directement à la passerelle Internet. Il s'agit d'une violation de la gestion des itinéraires. La correction suggérée dans ce cas peut être une liste d'actions ordonnées. La première est une recommandation d'ajouter les routes requises à la table de routage du sous-réseau Network Firewall afin de diriger le trafic sortant vers la passerelle Internet et de diriger le trafic entrant vers des destinations au sein du `local` VPC. La deuxième recommandation consiste à remplacer la route de passerelle Internet ou la route Network Firewall non valide dans la table de routage du sous-réseau pour diriger le trafic sortant vers les points de terminaison du pare-feu. La troisième recommandation consiste à ajouter les routes requises à la table de routage de la passerelle Internet pour diriger le trafic entrant vers les points de terminaison du pare-feu.

- **`AWS::EC2::InternetGateway`**— Ceci est utilisé pour les politiques de Network Firewall dans lesquelles le mode Monitor est activé.
  - Violations de gestion des itinéraires : la passerelle Internet n'est pas conforme si elle n'est pas associée à une table de routage ou si une route non valide figure dans la table de routage de la passerelle Internet.

- Actions de correction pour les violations de gestion des itinéraires : Firewall Manager suggère des actions correctives possibles pour remédier aux violations de gestion des itinéraires.

  Example 1 — Violation de la gestion des itinéraires et suggestions de mesures correctives

  Une passerelle Internet n'est pas associée à une table de routage. Les mesures correctives suggérées peuvent être une liste d'actions ordonnées. La première action consiste à créer une table de routage. La deuxième action consiste à associer la table de routage à la passerelle Internet. La troisième action consiste à ajouter la route requise à la table de routage de la passerelle Internet.

  Example 2 — Violation de la gestion des itinéraires et suggestions de mesures correctives

  La passerelle Internet est associée à une table de routage valide, mais la route n'est pas correctement configurée. La correction suggérée peut être une liste d'actions ordonnées. La première suggestion consiste à supprimer l'itinéraire non valide. La seconde consiste à ajouter la route requise à la table de routage de la passerelle Internet.

- **`AWS::NetworkFirewall::FirewallPolicy`**— Ceci est utilisé pour les politiques de Network Firewall. Firewall Manager affiche des informations sur une politique de pare-feu de Network Firewall qui a été modifiée de manière à la rendre non conforme. Les informations fournissent la politique de pare-feu attendue et la politique trouvée dans le compte client, afin que vous puissiez comparer les noms des groupes de règles apatrides et les paramètres de priorité, les noms d'actions personnalisés et les paramètres d'actions apatrides par défaut. Le composant de description de la violation contient une description de l'état attendu de la ressource, de l'état actuel non conforme et, le cas échéant, une description de la cause de l'écart.
- **`AWS::EC2::VPC`**— Ceci est utilisé pour les politiques de pare-feu DNS. Firewall Manager affiche des informations sur un VPC qui est concerné par une politique de pare-feu DNS de Firewall Manager et qui n'est pas conforme à cette politique. Les informations fournies incluent les groupes de règles attendus qui devraient être associés au VPC et les groupes de règles réels. Le composant de description de la violation contient une description de l'état attendu de la ressource, de l'état actuel non conforme et, le cas échéant, une description de la cause de l'écart.

AWS Firewall Manager résultats

AWS Firewall Manager crée des résultats pour les ressources non conformes et pour les attaques qu'il détecte, puis les envoie AWS Security Hub. Pour plus d'informations sur les résultats de Security Hub, consultez Findings in AWS Security Hub.

Lorsque vous utilisez Security Hub et Firewall Manager, Firewall Manager envoie automatiquement vos résultats à Security Hub. Pour plus d'informations sur la prise en main de Security Hub, consultez la section Configuration AWS Security Hub du guide de AWS Security Hub l'utilisateur.

> **Note**
>
> Firewall Manager ne met à jour les résultats que pour les politiques qu'il gère et pour les ressources qu'il surveille.
> Firewall Manager ne résout pas les problèmes suivants :
>
> - Politiques qui ont été supprimées.
> - Ressources qui ont été supprimées.
> - Ressources qui ont dépassé le champ d'application de la politique de Firewall Manager, par exemple en raison d'un changement de balise ou de définition de politique.

Comment puis-je consulter les résultats de mon Firewall Manager ?

Pour consulter les résultats de Firewall Manager dans Security Hub, suivez les instructions de la section Working with Findings in Security Hub et créez un filtre à l'aide des paramètres suivants :

- Attribut défini sur Product Name (Nom du produit).
- Opérateur défini sur EQUALS.
- Valeur définie sur `Firewall Manager`. Ce paramètre est sensible à la casse.

Puis-je désactiver cela ?

Vous pouvez désactiver l'intégration des AWS Firewall Manager résultats à Security Hub via la console Security Hub. Choisissez Integrations dans la barre de navigation, puis dans le volet Firewall Manager, choisissez Disable Integration. Pour plus d'informations, consultez le Guide de l'utilisateur AWS Security Hub.

AWS Firewall Manager types de recherche

- AWS WAF conclusions relatives aux politiques
- AWS Shield Advanced conclusions relatives aux politiques
- Résultats de la stratégie commune du groupe de sécurité
- Résultats de la stratégie d'audit du contenu du groupe de sécurité
- Résultats de la stratégie d'audit de l'utilisation du groupe de sécurité
- Conclusions relatives à la politique relative au pare-feu DNS d'Amazon Route 53 Resolver

AWS WAF conclusions relatives aux politiques

Vous pouvez utiliser AWS WAF les politiques de Firewall Manager pour appliquer des groupes de AWS WAF règles à vos ressources dans AWS Organizations. Pour plus d'informations, consultez Travailler avec les AWS Firewall Manager politiques.

La ressource est absente de l'ACL Web géré par Firewall Manager.

Une AWS ressource ne possède pas l'association ACL Web AWS Firewall Manager gérée conformément à la politique de Firewall Manager. Vous pouvez activer la correction de Firewall Manager sur la politique pour corriger ce problème.

- Sévérité : 80
- Paramètres d'état — RÉUSSI/ÉCHEC
- Mises à jour : si Firewall Manager exécute l'action corrective, le résultat sera mis à jour et la gravité diminuera de `HIGH` à`INFORMATIONAL`. Si vous effectuez la correction, Firewall Manager ne mettra pas à jour le résultat.

L'ACL Web géré par Firewall Manager a mal configuré les groupes de règles.

Les groupes de règles d'une ACL Web gérée par Firewall Manager ne sont pas correctement configurés, conformément à la politique de Firewall Manager. Cela signifie que les groupes de règles requis par la stratégie sont absents de la liste ACL web. Vous pouvez activer la correction de Firewall Manager sur la politique pour corriger ce problème.

- Sévérité : 80
- Paramètres d'état — RÉUSSI/ÉCHEC

- Mises à jour : si Firewall Manager exécute l'action corrective, le résultat sera mis à jour et la gravité diminuera de `HIGH` à`INFORMATIONAL`. Si vous effectuez la correction, Firewall Manager ne mettra pas à jour le résultat.

AWS Shield Advanced conclusions relatives aux politiques

Pour plus d'informations sur AWS Shield Advanced les politiques, consultezPolitiques des groupes de sécurité.

La ressource ne dispose pas de la protection Shield Advanced.

Une AWS ressource qui devrait bénéficier de la protection Shield Advanced, conformément à la politique de Firewall Manager, ne l'est pas. Vous pouvez activer la correction de Firewall Manager sur la politique, ce qui permettra de protéger la ressource.

- Sévérité : 60
- Paramètres d'état — RÉUSSI/ÉCHEC
- Mises à jour : si Firewall Manager exécute l'action corrective, le résultat sera mis à jour et la gravité diminuera de `HIGH` à`INFORMATIONAL`. Si vous effectuez la correction, Firewall Manager ne mettra pas à jour le résultat.

Shield Advanced a détecté une attaque contre une ressource surveillée.

Shield Advanced a détecté une attaque contre une AWS ressource protégée. Vous pouvez activer la correction de Firewall Manager sur la politique.

- Gravité — 70
- Paramètres d'état — Aucun
- Mises à jour — Firewall Manager ne met pas à jour ce résultat.

Résultats de la stratégie commune du groupe de sécurité

Pour de plus amples informations sur les stratégies communes des groupes de sécurité, veuillez consulter Politiques des groupes de sécurité.

La ressource a mal configuré le groupe de sécurité.

Firewall Manager a identifié une ressource qui ne possède pas les associations de groupes de sécurité gérés qu'elle devrait avoir, conformément à la politique de Firewall Manager. Vous pouvez activer la correction de Firewall Manager sur la politique, qui crée les associations en fonction des paramètres de stratégie.

- Gravité — 70
- Paramètres d'état — RÉUSSI/ÉCHEC
- Mises à jour — Firewall Manager met à jour cette constatation.

Le groupe de sécurité répliqué de Firewall Manager n'est pas synchronisé avec le groupe de sécurité principal.

Un groupe de sécurité répliqué de Firewall Manager n'est pas synchronisé avec son groupe de sécurité principal, conformément à leur politique de groupe de sécurité commune. Vous pouvez activer la correction de Firewall Manager sur la politique, qui synchronise les groupes de sécurité répliqués avec le groupe de sécurité principal.

- Sévérité : 80
- Paramètres d'état — RÉUSSI/ÉCHEC
- Mises à jour — Firewall Manager met à jour cette constatation.

Résultats de la stratégie d'audit du contenu du groupe de sécurité

Pour de plus amples informations sur les stratégies d'audit du contenu des groupes de sécurité, veuillez consulter Politiques des groupes de sécurité.

Le groupe de sécurité n'est pas conforme au groupe de sécurité d'audit de contenu.

Une politique d'audit du contenu du groupe de sécurité Firewall Manager a identifié un groupe de sécurité non conforme. Il s'agit d'un groupe de sécurité créé par le client qui se trouve dans la portée de la stratégie d'audit de contenu et qui ne respecte pas les paramètres définis par la stratégie et son groupe de sécurité d'audit. Vous pouvez activer la correction de Firewall Manager sur la politique, qui modifie le groupe de sécurité non conforme pour le mettre en conformité.

- Gravité — 70
- Paramètres d'état — RÉUSSI/ÉCHEC
- Mises à jour — Firewall Manager met à jour cette constatation.

Résultats de la stratégie d'audit de l'utilisation du groupe de sécurité

Pour de plus amples informations sur les stratégies d'audit d'utilisation des groupes de sécurité, veuillez consulter Politiques des groupes de sécurité.

Firewall Manager a détecté un groupe de sécurité redondant.

L'audit d'utilisation du groupe de sécurité Firewall Manager a identifié un groupe de sécurité redondant. Il s'agit d'un groupe de sécurité dont les règles sont identiques à celles d'un autre groupe de sécurité au sein de la même instance Amazon Virtual Private Cloud. Vous pouvez activer la correction automatique par Firewall Manager de la politique d'audit d'utilisation, qui remplace les groupes de sécurité redondants par un seul groupe de sécurité.

- Gravité — 30
- Paramètres d'état — Aucun
- Mises à jour — Firewall Manager ne met pas à jour ce résultat.

Firewall Manager a détecté un groupe de sécurité inutilisé.

L'audit d'utilisation du groupe de sécurité Firewall Manager a identifié un groupe de sécurité non utilisé. Il s'agit d'un groupe de sécurité qui n'est référencé par aucune politique de groupe de sécurité commune de Firewall Manager. Vous pouvez activer la correction automatique de Firewall Manager sur la politique d'audit d'utilisation, qui supprime les groupes de sécurité inutilisés.

- Gravité — 30
- Paramètres d'état — Aucun
- Mises à jour — Firewall Manager ne met pas à jour ce résultat.

Conclusions relatives à la politique relative au pare-feu DNS d'Amazon Route 53 Resolver

Pour plus d'informations sur les politiques de pare-feu DNS, consultezPolitiques de pare-feu DNS d'Amazon Route 53 Resolver.

La ressource est absente de la protection du pare-feu DNS

Il manque à un VPC une association de groupes de règles de pare-feu DNS définie dans la politique de pare-feu DNS de Firewall Manager. Le résultat répertorie le groupe de règles spécifié par la politique.

- Gravité — 80

Sécurité dans votre utilisation du AWS Firewall Manager service

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

> **Note**
>
> Cette section fournit des conseils AWS de sécurité standard pour votre utilisation du AWS Firewall Manager service et de ses AWS ressources, tels que les politiques de Firewall Manager Network Firewall et les politiques des groupes de sécurité.
> Pour plus d'informations sur la protection de vos AWS ressources à l'aide de Firewall Manager, consultez le reste du guide Firewall Manager.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cette notion par les termes sécurité du cloud et sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute les AWS services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. L'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Firewall Manager, consultez la section AWS Services concernés par programme de conformité.
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre organisation ainsi que les lois et réglementations applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de Firewall Manager. Les rubriques suivantes expliquent comment configurer Firewall Manager pour répondre à vos objectifs de sécurité et de conformité. Vous

apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos ressources Firewall Manager.

Rubriques

Protection des données dans Firewall Manager

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Firewall Manager. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour en savoir plus sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l’authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.

- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour en savoir plus sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Firewall Manager ou un autre outil Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous saisissez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Les entités Firewall Manager, telles que les politiques, sont chiffrées au repos, sauf dans certaines régions où le chiffrement n'est pas disponible, notamment en Chine (Pékin) et en Chine (Ningxia). Des clés de chiffrement uniques sont utilisées pour chaque région.

Identity and Access Management pour AWS Firewall Manager

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources de Firewall Manager. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

- Résolution des problèmes AWS Firewall Manager d'identité et d'accès
- Utilisation de rôles liés à un service pour Firewall Manager
- Prévention du problème de l’adjoint confus entre services

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Firewall Manager.

Utilisateur du service : si vous utilisez le service Firewall Manager pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités de Firewall Manager pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Firewall Manager, consultezRésolution des problèmes AWS Shield d'identité et d'accès.

Administrateur du service : si vous êtes responsable des ressources de Firewall Manager dans votre entreprise, vous disposez probablement d'un accès complet à Firewall Manager. C'est à vous de déterminer les fonctionnalités et les ressources de Firewall Manager auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d’IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec Firewall Manager, consultezComment AWS Shield fonctionne avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Firewall Manager. Pour consulter des exemples de politiques basées sur l'identité de Firewall Manager que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l’identité pour AWS Shield

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs

(IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent

des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour connaître la différence entre les rôles et les politiques basées sur les ressources pour l'accès entre comptes, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.

  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal

(utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de

confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS Firewall Manager fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Firewall Manager, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Firewall Manager.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Firewall Manager

Fonction IAM	Assistance pour Firewall Manager
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Non
Actions de politique	Oui

Fonction IAM	Assistance pour Firewall Manager
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Non
ACL	Non
ABAC (étiquettes dans les politiques)	Oui
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Fonctions du service	Partielle
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont Firewall Manager et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Firewall Manager

Prend en charge les politiques basées sur l'identité	Oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments

que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Pour consulter des exemples de politiques basées sur l'identité de Firewall Manager, consultez. Exemples de politiques basées sur l'identité pour AWS Firewall Manager

Exemples de politiques basées sur l'identité pour Firewall Manager

Pour consulter des exemples de politiques basées sur l'identité de Firewall Manager, consultez. Exemples de politiques basées sur l'identité pour AWS Firewall Manager

Politiques basées sur les ressources dans Firewall Manager

Prend en charge les politiques basées sur les ressources	Non

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal entre comptes à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez la section Accès aux ressources entre comptes dans IAM dans le guide de l'utilisateur d'IAM.

Actions de stratégie pour Firewall Manager

Prend en charge les actions de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une stratégie afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions de Firewall Manager, consultez la section Actions définies par AWS Firewall Manager dans le Service Authorization Reference.

Les actions de stratégie dans Firewall Manager utilisent le préfixe suivant avant l'action :

```
fms
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "fms:action1",
      "fms:action2"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Describe`, incluez l'action suivante :

```
"Action": "fms:Describe*"
```

Pour consulter des exemples de politiques basées sur l'identité de Firewall Manager, consultez. Exemples de politiques basées sur l'identité pour AWS Firewall Manager

Ressources relatives aux politiques pour Firewall Manager

Prend en charge les ressources de politique	Oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Firewall Manager et de leurs ARN, consultez la section Ressources définies par AWS Firewall Manager dans le Service Authorization Reference. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Firewall Manager.

Pour consulter des exemples de politiques basées sur l'identité de Firewall Manager, consultez. Exemples de politiques basées sur l'identité pour AWS Firewall Manager

Clés de conditions de politique pour Firewall Manager

Prend en charge les clés de condition de politique spécifiques au service	Non

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Pour consulter la liste des clés de condition de Firewall Manager, reportez-vous à la section Clés de condition correspondantes AWS Firewall Manager dans le Service Authorization Reference. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez la section Actions définies par AWS Firewall Manager.

Pour consulter des exemples de politiques basées sur l'identité de Firewall Manager, consultez. Exemples de politiques basées sur l'identité pour AWS Firewall Manager

ACL dans Firewall Manager

Prend en charge les listes ACL	Non

Les listes de contrôle d'accès (ACL) vérifient quels principaux (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux

politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

ABAC avec Firewall Manager

Prend en charge ABAC (étiquettes dans les politiques)	Oui

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur l'ABAC, consultez Qu'est-ce que le contrôle d'accès basé sur les attributs (ABAC) ? dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Firewall Manager

Prend en charge les informations d'identification temporaires	Oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent

avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Changement de rôle (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Transférer les sessions d'accès pour Firewall Manager

Prend en charge les sessions d'accès direct (FAS)	Oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Firewall Manager

Prend en charge les fonctions du service	Partielle

Une fonction de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités de Firewall Manager. Modifiez les rôles de service uniquement lorsque Firewall Manager fournit des instructions à cet effet.

Choix d'un rôle IAM dans Firewall Manager

Pour utiliser l'action *PutNotificationChannel*API dans Firewall Manager, vous devez choisir un rôle permettant à Firewall Manager d'accéder à Amazon SNS afin que le service puisse publier des messages Amazon SNS en votre nom. Pour plus d'informations, consultez PutNotificationChannella référence de AWS Firewall Manager l'API.

Voici un exemple de paramètre d'autorisation de rubrique SNS. Pour utiliser cette politique avec votre propre rôle personnalisé, remplacez le `AWSServiceRoleForFMS` Amazon Resource Name (ARN) par l'`SnsRoleName`ARN.

```
{
  "Sid": "AWSFirewallManagerSNSPolicy",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::account ID:role/aws-service-role/
fms.amazonaws.com/AWSServiceRoleForFMS"
  },
  "Action": "sns:Publish",
  "Resource": "SNS topic ARN"
}
```

Pour plus d'informations sur les actions et les ressources de Firewall Manager, consultez la rubrique du AWS Identity and Access Management guide Actions définies par AWS Firewall Manager

Rôles liés à un service pour Firewall Manager

Prend en charge les rôles liés à un service.	Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés à un service, consultez Services AWS qui fonctionnent avec IAM. Recherchez un service dans le tableau qui inclut un `Yes` dans la colonne Rôle lié à un service. Choisissez le lien Oui pour consulter la documentation du rôle lié à ce service.

Exemples de politiques basées sur l'identité pour AWS Firewall Manager

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier les ressources de Firewall Manager. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Firewall Manager, y compris le format des ARN pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition AWS Firewall Manager dans le Service Authorization Reference.

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Firewall Manager
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Accordez un accès en lecture à vos groupes de sécurité Firewall Manager

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Firewall Manager dans votre compte. Ces actions peuvent entraîner des frais pour

votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accorder les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation de IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utiliser des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez IAM Access Analyzer pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : IAM Access Analyzer valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger le MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Configuration de l'accès aux API protégé par MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Firewall Manager

Pour accéder à la AWS Firewall Manager console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher des informations détaillées sur les ressources de Firewall Manager de votre Compte AWS. Si vous créez une stratégie basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette stratégie.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent toujours utiliser la console Firewall Manager, associez également le Firewall Manager *ConsoleAccess* ou la politique *ReadOnly* AWS gérée aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
```

```
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accordez un accès en lecture à vos groupes de sécurité Firewall Manager

Firewall Manager autorise l'accès aux ressources entre comptes, mais il ne vous permet pas de créer des protections de ressources entre comptes. Vous pouvez uniquement créer des protections pour les ressources à partir du compte propriétaire de ces ressources.

Voici un exemple de politique qui accorde des autorisations pour les `fms:Getfms:List`, et les `ec2:DescribeSecurityGroups` actions sur toutes les ressources.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "fms:Get*",
                "fms:List*",
                "ec2:DescribeSecurityGroups"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

AWS politiques gérées pour AWS Firewall Manager

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée. AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d'informations, consultez la section Politiques gérées par AWS dans le Guide de l'utilisateur IAM.

AWS politique gérée : **`AWSFMAdminFullAccess`**

Utilisez la politique `AWSFMAdminFullAccess` AWS gérée pour permettre à vos administrateurs d'accéder aux AWS Firewall Manager ressources, y compris à tous les types de politiques de Firewall Manager. Cette politique n'inclut pas les autorisations pour configurer les notifications Amazon Simple Notification Service dans AWS Firewall Manager. Pour plus d'informations sur la configuration de l'accès pour Amazon Simple Notification Service, consultez Configuration de l'accès pour Amazon Simple Notification Service.

Pour la liste et les détails des politiques, consultez la console IAM à AWSFMAdminFullAccessl'adresse. Le reste de cette section donne un aperçu des paramètres de politique.

Déclarations d'autorisation

Cette politique est regroupée en déclarations en fonction de l'ensemble des autorisations.

- AWS Firewall Manager ressources de politique - Permet d'octroyer des autorisations administratives complètes aux ressources AWS Firewall Manager, y compris à tous les types de politiques de Firewall Manager.
- Écrire AWS WAF des journaux dans Amazon Simple Storage Service : permet à Firewall Manager d'écrire et de lire AWS WAF des journaux dans Amazon S3.
- Créer un rôle lié à un service : permet à l'administrateur de créer un rôle lié à un service, ce qui permet à Firewall Manager d'accéder aux ressources d'autres services en votre nom. Cette autorisation permet de créer le rôle lié à un service uniquement destiné à être utilisé par Firewall Manager. Pour plus d'informations sur la manière dont Firewall Manager utilise les rôles liés à un service, consultez. Utilisation de rôles liés à un service pour Firewall Manager
- AWS Organizations— Permet aux administrateurs d'utiliser Firewall Manager pour une organisation dans AWS Organizations. Après avoir activé l'accès sécurisé pour Firewall Manager dans AWS Organizations, les membres du compte administrateur peuvent consulter les résultats au sein de leur organisation. Pour plus d'informations sur l'utilisation AWS Organizations avec AWS Firewall Manager, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans le Guide de AWS Organizations l'utilisateur.

Catégories d'autorisations

La liste suivante répertorie les types d'autorisations prévus dans la politique et les autorisations qu'elles fournissent.

- `fms`— Travaillez avec AWS Firewall Manager les ressources.
- `waf`et `waf-regional` — Travaillez avec les politiques AWS WAF classiques.
- `elasticloadbalancing`— Associez des AWS WAF ACL Web à des équilibreurs de charge élastiques.
- `firehose`— Afficher les informations relatives AWS WAF aux journaux.
- `organizations`— Travaillez avec les ressources AWS des Organizations.
- `shield`— Consultez l'état des AWS Shield politiques d'abonnement.
- `route53resolver`— Travaillez avec les groupes de règles Route 53 Private DNS pour VPC dans le cadre d'une politique Route 53 Private DNS pour VPC.
- `wafv2`— Travaillez avec des AWS WAFV2 politiques.
- `network-firewall`— Travaillez avec des AWS Network Firewall politiques.
- `ec2`— Afficher les zones de disponibilité et les régions de la politique.

- `s3`— Afficher les informations relatives AWS WAF aux journaux.

AWS politique gérée : **`FMSServiceRolePolicy`**

Cette politique permet AWS Firewall Manager de gérer les AWS ressources en votre nom dans Firewall Manager et dans les services intégrés. Cette politique est attachée au rôle lié à un service `AWSServiceRoleForFMS`. Pour de plus amples informations sur le rôle lié à un service, veuillez consulter Utilisation de rôles liés à un service pour Firewall Manager.

Pour plus de détails sur les politiques, consultez la console IAM de ServiceRolePolicyFMS.

AWS politique gérée : AWSFMAdminReadOnlyAccess

Accorde un accès en lecture seule à toutes les ressources de AWS Firewall Manager.

Pour la liste et les détails des politiques, consultez la console IAM à AWSFMAdminReadOnlyAccessl'adresse. Le reste de cette section donne un aperçu des paramètres de politique.

Catégories d'autorisations

La liste suivante répertorie les types d'autorisations prévus dans la politique et les informations auxquelles les autorisations autorisent un accès en lecture seule.

- `fms`— AWS Firewall Manager ressources.
- `waf`et `waf-regional` — Politiques AWS WAF classiques.
- `firehose`— AWS WAF journaux.
- `organizations`— Ressources pour AWS les organisations.
- `shield`— AWS Shield politiques.
- `route53resolver`— Groupes de règles de DNS privé Route 53 pour VPC dans le cadre d'une politique de DNS privé Route 53 pour VPC.
- `wafv2`— Vos AWS WAFV2 groupes de règles et les groupes de règles AWS gérées disponibles dans AWS WAFV2.
- `network-firewall`— les groupes de AWS Network Firewall règles et les métadonnées des groupes de règles.
- `ec2`— AWS Network Firewall politique Zones de disponibilité et régions.
- `s3`— AWS WAF journaux.

AWS politique gérée : AWSFMMemberReadOnlyAccess

Accorde un accès en lecture seule aux ressources des AWS Firewall Manager membres. Pour la liste et les détails des politiques, consultez la console IAM à AWSFMMemberReadOnlyAccessl'adresse.

Mises à jour des politiques AWS gérées par Firewall Manager

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Firewall Manager depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des documents de Firewall Manager à l'adresseHistorique du document.

Modification	Description	Date
FMS ServiceRolePolicy — Politique mise à jour	Autorisations ajoutées pour la gestion des ACL réseau. Consultez la politique mise à jour dans la console IAM : ServiceRolePolicyFMS.	2024-04-22
FMS ServiceRolePolicy — Politique mise à jour	Des autorisations ont été ajoutées qui permettent à Firewall Manager de décrire si les AWS Config règles spécifiées sont conformes. Consultez la politique mise à jour dans la console IAM : ServiceRolePolicyFMS.	21/04/2023
FMS ServiceRolePolicy — Politique mise à jour	Autorisations ajoutées qui permettent à Firewall Manager de décrire les attributs de	15 novembre

Modification	Description	Date
	l'instance Amazon EC2 et de l'interface réseau. Consultez la politique mise à jour dans la console IAM : ServiceRolePolicyFMS.	
AWSFMAdminReadOnly Access— Politique mise à jour	Ajout d'autorisations pour le support AWS WAFV2, le Shield, le Network Firewall, le pare-feu DNS, le groupe de sécurité Amazon VPC, les politiques. Consultez la politique mise à jour dans la console IAM : AWSFMAdminReadOnly Access.	02/11/11
AWSFMAdminFullAccess— Politique mise à jour	Ajout d'autorisations pour le support AWS WAFV2, le Shield, le Network Firewall, le pare-feu DNS, le groupe de sécurité Amazon VPC, les politiques. Autorisations Amazon SNS supprimées. Consultez la politique mise à jour dans la console IAM : AWSFMAdminFullAccess.	21/10/10

Modification	Description	Date
`FMSServiceRolePolicy` — Nouvelles autorisations pour les politiques de pare-feu AWS Firewall Manager tierces	Cette modification permet à Firewall Manager de créer et de supprimer les points de terminaison Amazon EC2 VPC associés à une politique de pare-feu tierce.	30/03/2018
`FMSServiceRolePolicy` — Nouvelles autorisations pour les AWS Network Firewall politiques	Ajout de nouvelles autorisations pour prendre en charge le déploiement de pare-feux pour les politiques de Network Firewall. Les nouvelles autorisations permettent de récupérer des informations sur les zones de disponibilité pour les comptes concernés par une politique.	16/02/02
`FMSServiceRolePolicy` — Nouvelles autorisations pour les AWS Shield politiques	Ajout de nouvelles autorisations permettant de récupérer des balises pour les ressources AWS WAF régionales et AWS WAF mondiales. Des autorisations AWS WAF régionales ont été ajoutées pour récupérer des ACL Web à l'aide d'un ARN de ressource. Des autorisations ont été ajoutées pour prendre en charge l'atténuation automatique des attaques DDoS au niveau de la couche applicative Shield.	07/01/2018

Modification	Description	Date
`FMSServiceRolePolicy` — Nouvelles autorisations pour les AWS Shield politiques	Ajout d'une nouvelle autorisation permettant de récupérer des balises pour les ressources Elastic Load Balancing.	18/11/2021
`FMSServiceRolePolicy` — Nouvelles autorisations pour les groupes de sécurité et AWS Network Firewall les politiques	Ajout de nouvelles autorisations pour permettre la journalisation centralisée des AWS Network Firewall politiques. En outre, des autorisations Amazon EC2 en lecture seule ont été ajoutées pour prendre en charge les modifications apportées au service Config qui ont un impact sur la AWS Firewall Manager manière dont les ressources sont demandées pour les politiques des groupes de sécurité.	2021-09-29
`FMSServiceRolePolicy` — Formats ARN pour les AWS WAF ressources	Mise à jour du `FMSServiceRolePolicy` afin de standardiser les formats d'ARN pour les AWS WAF ressources. Les formats ARN mis à jour sont `arn:aws:waf:*:*:*` et`arn:aws:waf-regional:*:*:*` .	12/08/2021
`FMSServiceRolePolicy` — Autres régions en Chine	AWS Firewall Manager a été activé `FMSServiceRolePolicy` pour les régions BJS et ZHY en Chine.	12/08/2021

Modification	Description	Date
`FMSServiceRolePolicy` — Mise à jour de la politique existante	Ajout de nouvelles autorisations permettant AWS Firewall Manager de gérer le pare-feu Amazon Route 53 Resolver DNS. Cette modification permet à Firewall Manager de configurer les associations de pare-feu Amazon Route 53 Resolver DNS. Cela vous permet d'utiliser Firewall Manager pour fournir des protections de pare-feu DNS à vos VPC dans l'ensemble de votre organisation dans AWS Organizations.	17/03/2021
Firewall Manager a commencé à suivre les modifications	Firewall Manager a commencé à suivre les modifications apportées AWS à ses politiques gérées.	02/03/2021

Résolution des problèmes AWS Firewall Manager d'identité et d'accès

Utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation de Firewall Manager et d'IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Firewall Manager
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources de mon Firewall Manager

Je ne suis pas autorisé à effectuer une action dans Firewall Manager

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `fms:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fms:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `fms:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer cette `iam:PassRole` action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Firewall Manager.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Firewall Manager. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les stratégies de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à moi Compte AWS à accéder aux ressources de mon Firewall Manager

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si Firewall Manager prend en charge ces fonctionnalités, consultezComment AWS Shield fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Utilisation de rôles liés à un service pour Firewall Manager

AWS Firewall Manager utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Firewall Manager. Les rôles liés aux services sont prédéfinis par Firewall Manager et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration de Firewall Manager car il n'est pas nécessaire d'ajouter manuellement les autorisations nécessaires. Firewall Manager définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul Firewall Manager peut

assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisations. Cette politique d'autorisations ne peut pas être attachée à une autre entité IAM.

Vous ne pouvez supprimer un rôle lié à un service qu'après avoir supprimé les ressources connexes du rôle. Cela protège les ressources de votre Firewall Manager car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées à un service pour Firewall Manager

AWS Firewall Manager utilise le nom du rôle lié au service AWSServiceRoleForFMS pour permettre à Firewall Manager d'appeler AWS des services en votre nom afin de gérer les politiques de pare-feu et les ressources du AWS Organizations compte. Cette politique est associée au rôle AWS géré`AWSServiceRoleForFMS`. Pour plus d'informations sur le rôle géré, consultezAWS politique gérée : `FMSServiceRolePolicy`.

Le rôle AWSServiceRoleForFMS lié au service fait confiance au service pour assumer le rôle. `fms.amazonaws.com`

La politique d'autorisation des rôles permet à Firewall Manager d'effectuer les actions suivantes sur les ressources spécifiées :

- `waf`- Gérez les ACL Web AWS WAF classiques, les autorisations des groupes de règles et les associations d'ACL Web dans votre compte.
- `ec2`- Gérez les groupes de sécurité sur les interfaces réseau élastiques et les instances Amazon EC2. Gérez les ACL réseau sur les sous-réseaux Amazon VPC.
- `vpc`- Gérez les sous-réseaux, les tables de routage, les balises et les points de terminaison dans Amazon VPC.
- `wafv2`- Gérez les ACL AWS WAF Web, les autorisations des groupes de règles et les associations d'ACL Web dans votre compte.
- `cloudfront`- Créez des ACL Web pour protéger les CloudFront distributions.
- `config`- Gérez les AWS Config règles propres à Firewall Manager dans votre compte.
- `iam`- Gérez ce rôle lié au service et créez les rôles obligatoires et liés au service AWS WAF Shield si vous configurez les politiques de journalisation et AWS WAF de Shield.

- `organization`- Créez un rôle lié à un service appartenant à Firewall Manager pour gérer les AWS Organizations ressources utilisées par Firewall Manager.
- `shield`- Gérez les AWS Shield protections et les configurations d'atténuation L7 pour les ressources de votre compte.
- `ram`- Gérez le partage AWS RAM des ressources pour les groupes de règles du pare-feu DNS et les groupes de règles du pare-feu réseau.
- `network-firewall`- Gérez les AWS Network Firewall ressources appartenant à Firewall Manager et les ressources Amazon VPC dépendantes de votre compte.
- `route53resolver`- Gérez les associations de pare-feu DNS appartenant à Firewall Manager dans votre compte.

Consultez la politique complète dans la console IAM : ServiceRolePolicyFMS.

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le IAM User Guide (guide de l'utilisateur IAM).

Création d'un rôle lié à un service pour Firewall Manager

Vous n’avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous activez la connexion de Firewall Manager sur le AWS Management Console, ou que vous faites une `PutLoggingConfiguration` demande dans la CLI de Firewall Manager ou dans l'API Firewall Manager, Firewall Manager crée le rôle lié au service pour vous.

Vous devez disposez de l'autorisation `iam:CreateServiceLinkedRole` pour activer la journalisation.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous activez la journalisation de Firewall Manager, Firewall Manager crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour Firewall Manager

Firewall Manager ne vous permet pas de modifier le rôle AWSServiceRoleForFMS lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du

rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Firewall Manager

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

> **Note**
>
> Si le service Firewall Manager utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM, la CLI IAM ou l'API IAM pour supprimer le rôle lié au AWSServiceRoleForFMS service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés au service Firewall Manager

Firewall Manager prend en charge l'utilisation de rôles liés à un service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez la section Points de terminaison et quotas de Firewall Manager.

Prévention du problème de l'adjoint confus entre services

Le problème de l'adjoint confus est un problème de sécurité dans lequel une entité qui n'a pas l'autorisation d'effectuer une action peut contraindre une entité plus privilégiée à effectuer cette action. En AWS, l'usurpation d'identité interservices peut entraîner un problème de confusion chez les adjoints. L'usurpation d'identité entre services peut se produire lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Le service appelant peut être manipulé et ses autorisations utilisées pour agir sur les ressources d'un autre client auxquelles on ne serait pas autorisé d'accéder autrement. Pour éviter cela, AWS fournit des outils qui vous aident à protéger vos données pour tous les services avec des principaux de service qui ont eu accès aux ressources de votre compte.

Nous recommandons d'utiliser les clés de contexte de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés contextuelles dans les politiques de ressources afin de limiter les autorisations qui AWS Firewall Manager accordent un autre service à la ressource. Utilisez `aws:SourceArn` si vous souhaitez qu'une seule ressource soit associée à l'accès entre services. Utilisez `aws:SourceAccount` si vous souhaitez autoriser l'association d'une ressource de ce compte à l'utilisation interservices.

Le moyen le plus efficace de se protéger du problème de l'adjoint désorienté consiste à utiliser la clé de contexte de condition globale `aws:SourceArn` avec l'ARN complet de la ressource. Si vous ne connaissez pas l'ARN complet de la ressource ou si vous spécifiez plusieurs ressources, utilisez la clé de contexte de condition globale `aws:SourceArn` avec des caractères génériques (`*`) pour les parties inconnues de l'ARN. Par exemple, `arn:aws:fms:*:`*`account-id`*`:*`.

Si la valeur `aws:SourceArn` ne contient pas l'ID du compte, tel qu'un ARN de compartiment Amazon S3, vous devez utiliser les deux clés de contexte de condition globale pour limiter les autorisations.

La valeur de `aws:SourceArn` doit être le AWS compte de l' AWS Firewall Manager administrateur.

Les exemples suivants montrent comment utiliser la clé de contexte de condition `aws:SourceArn` globale dans Firewall Manager pour éviter le problème de confusion des adjoints.

L'exemple suivant montre comment éviter le problème de confusion des adjoints en utilisant la clé de contexte de condition `aws:SourceArn` globale dans la politique de confiance des rôles de Firewall Manager. Remplacez *`la région`* et l'*`identifiant du compte`* par vos propres informations.

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

Journalisation et surveillance dans Firewall Manager

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de Firewall Manager et de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. AWS fournit plusieurs outils pour surveiller les ressources de votre Firewall Manager et répondre à des événements potentiels :

CloudWatch Alarmes Amazon

À l'aide d' CloudWatch alarmes, vous observez une seule métrique sur une période que vous spécifiez. Si la métrique dépasse un seuil donné, CloudWatch envoie une notification à une rubrique ou AWS Auto Scaling à une politique Amazon SNS. Pour plus d’informations, consultez Surveillance avec Amazon CloudWatch.

AWS CloudTrail Journaux

CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Firewall Manager. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Firewall Manager, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires. Pour plus d'informations, voir Journalisation des appels d'API AWS CloudTrail avec.

Validation de conformité pour Firewall Manager

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et fournissent des étapes pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

  > **Note**
  >
  > Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.

- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans Firewall Manager

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone de disponibilité à l'autre sans interruption. Les zones de disponibilité sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Sécurité de l’infrastructure dans AWS Firewall Manager

En tant que service géré, AWS Firewall Manager il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Firewall Manager via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

AWS Firewall Manager quotas

AWS Firewall Manager est soumis aux quotas suivants (anciennement appelés limites).

AWS Firewall Manager possède des quotas par défaut que vous pourriez être en mesure d'augmenter et des quotas fixes.

Les politiques de groupe de sécurité et les politiques ACL réseau gérées par Firewall Manager sont soumises aux quotas Amazon VPC standard. Pour plus d'informations, consultez Amazon VPC Quotas dans le guide de l'utilisateur Amazon VPC.

Chaque politique de Firewall Manager Network Firewall crée un pare-feu Network Firewall associé à une stratégie de pare-feu et à ses groupes de règles. Ces ressources Network Firewall sont soumises aux quotas répertoriés dans la section AWS Network Firewall quotas du Network Firewall Developer Guide.

Quotas souples

AWS Firewall Manager dispose de quotas par défaut sur le nombre d'entités par région. Vous pouvez demander une augmentation de ces quotas.

Tous les types de politiques

Ressource	Quota par défaut par région
Comptes par organisation en AWS Organizations	Variable. Une invitation envoyée à un compte est comptabilisée par rapport à ce quota. Elle est décomptée si le compte invité décline l'invitation, si le compte de gestion annule l'invitation ou si celle-ci expire.
Politiques de Firewall Manager par organisation dans AWS Organizations.	50. Les spécifications `Global` de la région `US East (N. Virginia) Region` font référence à la même région, de sorte que cette limite s'applique au total des politiques combinées pour les deux.
Unités organisationnelles concernées par la politique de Firewall Manager.	20
Comptes concernés par une politique de Firewall Manager si vous incluez et excluez explicitement des comptes individuels.	200
Comptes concernés par une politique de Firewall Manager si vous n'incluez ou n'excluez pas explicitement des comptes individuels.	2 500

Ressource	Quota par défaut par région
Balises qui incluent ou excluent des ressources conformément à la politique de Firewall Manager.	8
Nombre d'ensembles de ressources par compte.	20
Nombre de ressources par ensemble de ressources.	100
Nombre de ressources définies par politique de Firewall Manager.	5

AWS WAF politiques

Ressource	Quota par défaut par région
AWS WAF groupes de règles par compte administrateur de Firewall Manager.	100
AWS WAF Groupes de règles classiques par compte administrateur de Firewall Manager.	10
Groupes de règles par AWS WAF politique.	50

Stratégies de groupe de sécurité communes

Ressource	Quota par défaut par région.
Principaux groupes de sécurité par politique.	3
Instances Amazon VPC couvertes par politique et par compte, y compris les VPC partagés.	100

Stratégies de groupe de sécurité d'audit de contenu

Ressource	Quota par défaut par région
Auditez les groupes de sécurité par stratégie.	1
Candidatures par liste de candidatures.	50
Listes d'applications gérées personnalisées pour les règles autorisant l'ensemble du trafic.	1
Listes d'applications gérées personnalisées conformément aux règles de politique.	1
Listes d'applications gérées personnalisées par compte.	10
Protocoles par liste de protocoles.	5
Listes de protocoles gérés personnalisées pour tous les paramètres d'une politique.	1
Listes de protocoles gérés personnalisés par compte.	10

Politiques ACL du réseau

Ressource	Quota par défaut par région
Nombre de règles entrantes par politique ACL réseau, utilisées pour les premières ou les dernières règles. Par exemple, vous pouvez avoir 5 premières règles et 0 dernières règles entrantes, ou 2 premières et 3 dernières, mais vous ne pouvez pas avoir 4 premières et 2 dernières.	5
Nombre de règles sortantes par politique ACL réseau, utilisées pour les premières ou les dernières règles. Par exemple, vous pouvez avoir 5 premières règles de sortie et 0 dernière, ou 2 premières et 3 dernières, mais vous ne pouvez pas avoir 4 premières et 2 dernières.	5

Politiques de pare-feu DNS

Ressource	Quota par défaut par région
Groupes de règles de pare-feu DNS conformément à la politique de pare-feu DNS.	2

Quotas stricts

Les quotas par région suivants relatifs à ne AWS Firewall Manager peuvent pas être modifiés.

Tous les types de politiques

Ressource	Quota par région
Le nombre maximum d'administrateurs Firewall Manager que vous pouvez avoir dans une AWS Organizations organisation. Vous devez avoir un administrateur par défaut et jusqu'à neuf administrateurs Firewall Manager supplémentaires.	10

AWS WAF politiques

Ressource	Quota par région
Nombre total d'unités de capacité de liste ACL web (WCU) pour les groupes de règles dans une stratégie AWS WAF .	5 000

AWS WAF Politiques classiques

Ressource	Quota par région
AWS WAF Groupes de règles classiques par politique.	2 : 1 groupe de règles créé par le client et 1 groupe de AWS Marketplace règles.

Ressource	Quota par région
AWS WAF Règles classiques par groupe de règles Firewall Manager AWS WAF Classic.	10

Politiques d'audit du contenu des groupes de sécurité

Ressource	Quota par région
Firewall Manager gérait des listes d'applications pour tous les paramètres d'une politique.	1
Firewall Manager gère des listes de protocoles pour tous les paramètres d'une politique.	1

Politiques de Network Firewall

Ressource	Quota par région
Nombre de VPC qui peuvent être corrigés automatiquement pour une seule politique.	1 000
Le nombre de CIDR IPV4 que vous pouvez fournir pour une seule politique.	50

Surveillance AWS WAFAWS Firewall Manager, et AWS Shield Advanced

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances de vos services.

> **Note**
>
> Pour plus d'informations sur la surveillance de vos ressources Shield Advanced et l'identification d'éventuels événements DDoS à l'aide de Shield Advanced, consultezAWS Shield.

Lorsque vous commencez à surveiller ces services, vous devez créer un plan de surveillance qui contient les réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

L'étape suivante consiste à établir une référence de performances normales d'un dans votre environnement, en mesurant la performance à divers moments et dans diverses conditions de charge. Pendant que vous surveillez AWS WAF, Firewall Manager, Shield Advanced et les services associés stockent les données de surveillance historiques afin que vous puissiez les comparer aux données de performance actuelles, identifier les modèles de performances normaux et les anomalies de performance, et concevoir des méthodes pour résoudre les problèmes.

En AWS WAF effet, vous devez au minimum surveiller les éléments suivants afin d'établir une base de référence :

- Nombre de requêtes Web autorisées
- Nombre de requêtes Web bloquées

Rubriques

Outils de surveillance

AWS fournit divers outils que vous pouvez utiliser pour surveiller AWS WAF et AWS Shield Advanced. Vous pouvez configurer certains de ces outils pour qu'ils effectuent la surveillance automatiquement, tandis que d'autres nécessitent une intervention manuelle. Nous vous recommandons d’automatiser le plus possible les tâches de supervision.

Outils de surveillance automatique

Vous pouvez utiliser les outils de surveillance automatique suivants pour surveiller AWS WAF AWS Shield Advanced et signaler tout problème :

- Tableaux de bord d'aperçu du trafic Web ACL : accédez aux résumés du trafic Web évalué par une ACL Web en accédant à la page de l'ACL Web dans la AWS WAF console et en ouvrant l'onglet Aperçu du trafic.

  Les tableaux de bord d'aperçu du trafic fournissent des résumés en temps quasi réel des CloudWatch métriques AWS WAF collectées par Amazon lors de l'évaluation du trafic Web de votre application. Vous pouvez consulter des résumés de l'ensemble de votre trafic Web et du trafic évalué par les groupes de règles d'atténuation intelligente des menaces.

  Pour plus d'informations, consultez Tableaux de bord de présentation du trafic Web ACL ou accédez aux tableaux de bord de la console.
- Amazon CloudWatch Alarms — Surveillez une seule métrique sur une période que vous spécifiez et effectuez une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. L’action est une notification envoyée à une rubrique Amazon Simple Notification Service (Amazon SNS) ou une politique Amazon EC2 Auto Scaling. Les alarmes déclenchent des actions uniquement pour les changements d'état prolongés. CloudWatch les alarmes ne déclencheront pas d'actions simplement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes. Pour plus d'informations, consultez la section Surveillance de CloudFront l'activité à l'aide de CloudWatch.

> **Note**
>
> CloudWatch les métriques et les alarmes ne sont pas activées pour AWS Firewall Manager.

Vous pouvez non seulement les utiliser CloudWatch pour surveiller AWS WAF et protéger les métriques avancées comme décrit dans la sectionSurveillance avec Amazon CloudWatch, mais vous devez également les utiliser CloudWatch pour surveiller l'activité de vos ressources protégées. Pour plus d'informations, consultez les ressources suivantes :

- Surveillance de CloudFront l'activité CloudWatch à l'aide du manuel Amazon CloudFront Developer Guide
- Journalisation et surveillance dans Amazon API Gateway dans le guide du développeur d'API Gateway
- CloudWatch Indications relatives à votre application Load Balancer dans le guide de l'utilisateur d'Elastic Load Balancing
- Surveillance et journalisation dans le guide du AWS AppSync développeur
- Journalisation et surveillance dans Amazon Cognito dans le manuel du développeur Amazon Cognito
- Affichage des logs App Runner transmis à CloudWatch Logs et affichage des statistiques du service App Runner indiquées CloudWatch dans le Guide du AWS App Runner développeur

- Amazon CloudWatch Logs — Surveillez, stockez et accédez à vos fichiers journaux depuis AWS CloudTrail ou d'autres sources. Pour plus d'informations, consultez Qu'est-ce qu'Amazon CloudWatch Logs ? .
- Amazon CloudWatch Events — Automatisez vos AWS services et répondez automatiquement aux événements du système. Les événements issus AWS des services sont transmis à CloudWatch Events en temps quasi réel, et vous pouvez spécifier des actions automatisées à effectuer lorsqu'un événement correspond à une règle que vous avez écrite. Pour plus d'informations, consultez Qu'est-ce qu'Amazon CloudWatch Events ?
- AWS CloudTrail Surveillance des journaux : partagez des fichiers journaux entre comptes, surveillez les fichiers CloudTrail journaux en temps réel en les envoyant à CloudWatch Logs, écrivez des applications de traitement des journaux en Java et vérifiez que vos fichiers journaux n'ont pas changé après leur livraison par. CloudTrail Pour plus d'informations, reportez-vous à

Journalisation des appels d'API AWS CloudTrail avec la section Utilisation des fichiers CloudTrail journaux dans le Guide de AWS CloudTrail l'utilisateur.

- AWS Config— Consultez la configuration des AWS ressources de votre AWS compte, y compris la façon dont les ressources sont liées les unes aux autres et comment elles ont été configurées dans le passé, afin de voir comment les configurations et les relations évoluent au fil du temps.

Outils de surveillance manuelle

Un autre élément important de AWS WAF la surveillance AWS Shield Advanced consiste à surveiller manuellement les éléments non couverts par les CloudWatch alarmes. Vous pouvez consulter le tableau de bord AWS WAF, Shield Advanced et d'autres AWS Management Console tableaux de bord pour connaître l'état de votre AWS environnement. CloudWatch Nous vous recommandons également de vérifier les fichiers journaux de vos ACL et règles Web.

- Par exemple, pour consulter le AWS WAF tableau de bord :
  - Dans l'onglet Demandes de la page AWS WAF Web ACL, visualisez un graphique du nombre total de demandes et de demandes correspondant à chaque règle que vous avez créée. Pour plus d’informations, consultez Affichage d'un exemple de demandes web.
- Consultez la page CloudWatch d'accueil pour les informations suivantes :
  - Alarmes et statuts en cours
  - Graphiques des alarmes et des ressources
  - Statut d’intégrité du service

  En outre, vous pouvez utiliser CloudWatch pour effectuer les opérations suivantes :
  - Créer des tableaux de bord personnalisés pour surveiller les services qui vous intéressent.
  - Données de métriques de graphiques pour résoudre les problèmes et découvrir les tendances.
  - Recherchez et parcourez tous les indicateurs de vos AWS ressources.
  - Créer et Modifier des alarmes pour être informé des problèmes.

Surveillance avec Amazon CloudWatch

Vous pouvez surveiller les requêtes Web, les ACL et les règles du Web à l'aide d'Amazon CloudWatch, qui collecte et traite les données brutes à partir de AWS WAF métriques lisibles AWS Shield Advanced en temps quasi réel. Vous pouvez utiliser les statistiques CloudWatch d'Amazon

pour avoir une idée des performances de votre application ou service Web. Pour plus d'informations, consultez le contenu CloudWatch du guide de CloudWatch l'utilisateur Amazon.

> **Note**
>
> CloudWatch les métriques et les alarmes ne sont pas activées pour Firewall Manager.

Vous pouvez créer une CloudWatch alarme Amazon qui envoie un message Amazon SNS lorsque l'alarme change d'état. Une alarme surveille une métrique individuelle pendant une période que vous définissez, et exécute une ou plusieurs actions en fonction de la valeur de cette métrique, par rapport à un seuil spécifié sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon SNS ou à une politique Auto Scaling. Les alarmes déclenchent des actions uniquement pour les changements d'état prolongés. CloudWatch les alarmes n'appellent pas d'actions simplement parce qu'elles sont dans un état particulier ; l'état doit avoir changé et être maintenu pendant un certain nombre de périodes.

Rubriques

Affichage des métriques et dimensions

Les métriques sont regroupées d'abord en fonction de l'espace de noms du service, puis en fonction des différentes combinaisons de dimensions au sein de chaque espace de noms. AWS Firewall Manager n'enregistre pas les métriques.

- L' AWS WAF espace de noms est `AWS/WAFV2`
- L'espace de noms Shield Advanced est `AWS/DDoSProtection`

> **Note**
>
> AWS WAF rapporte les statistiques une fois par minute.

Shield Advanced publie des statistiques une fois par minute lors d'un événement et moins fréquemment à d'autres moments.

Utilisez les procédures suivantes pour afficher les métriques pour AWS WAF et AWS Shield Advanced.

Pour afficher les métriques à l'aide de la CloudWatch console

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Si nécessaire, remplacez la région par celle où se trouvent vos AWS ressources. Pour CloudFront, choisissez la région USA Est (Virginie du Nord).
3. Dans le volet de navigation, sous Mesures, choisissez Toutes les mesures, puis recherchez le service dans l'onglet Parcourir.

Pour afficher les métriques à l'aide de la AWS CLI

- Pour AWS/WAFV2, à l'invite de commande, utilisez la commande suivante :

```
aws cloudwatch list-metrics --namespace "AWS/WAFV2"
```

  Pour Shield Advanced, à l'invite de commande, utilisez la commande suivante :

```
aws cloudwatch list-metrics --namespace "AWS/DDoSProtection"
```

AWS WAF métriques et dimensions

AWS WAF rapporte les statistiques une fois par minute. AWS WAF fournit des métriques et des dimensions dans l'espace de `AWS/WAFV2` noms.

Vous pouvez consulter les informations récapitulatives des AWS WAF métriques via la AWS WAF console, dans l'onglet d'aperçu du trafic de l'ACL Web. Pour plus d'informations, accédez à la console ou consultezTableaux de bord de présentation du trafic Web ACL.

Vous pouvez consulter les mesures suivantes pour les ACL, les règles, les groupes de règles et les étiquettes Web.

- Vos règles : les métriques sont regroupées en fonction de l'action de la règle. Par exemple, lorsque vous testez une règle en Count mode, ses correspondances sont répertoriées sous forme de `Count` métriques pour l'ACL Web.
- Vos groupes de règles : les statistiques de vos groupes de règles sont répertoriées sous les métriques des groupes de règles.
- Groupes de règles appartenant à un autre compte : les statistiques des groupes de règles ne sont généralement visibles que par le propriétaire du groupe de règles. Toutefois, si vous annulez l'action d'une règle, les mesures associées à cette règle seront répertoriées sous les mesures de votre ACL Web. En outre, les étiquettes ajoutées par n'importe quel groupe de règles sont répertoriées dans vos métriques ACL Web

  Les groupes de règles de cette catégorie sont les groupes de règles AWS Règles gérées pour AWS WAF AWS Marketplace groupes de règles gérésGroupes de règles fournis par d'autres services,, et les groupes de règles partagés avec vous par un autre compte.
- Étiquettes : les étiquettes qui ont été ajoutées à une demande Web lors de l'évaluation sont répertoriées dans les métriques des étiquettes ACL Web. Vous pouvez accéder aux statistiques de toutes les étiquettes, qu'elles aient été ajoutées par vos règles et groupes de règles ou par les règles d'un groupe de règles appartenant à un autre compte.

Rubriques

ACL Web, groupe de règles et mesures et dimensions

ACL Web, groupe de règles et métriques de règles

Métrique	Description
`AllowedRequests`	Nombre de requêtes Web autorisées. Critères de notification : il existe une valeur différente de zéro.

Métrique	Description
	Statistiques valides : somme
`BlockedRequests`	Nombre de requêtes Web bloquées. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`CountedRequests`	Nombre de requêtes Web comptabilisées. Critères de notification : il existe une valeur différente de zéro. Une demande web comptée est une demande qui correspond à au moins l'une des règles. Le comptage des demandes est généralement utilisé pour les tests. Statistiques valides : somme
`CaptchaRequests`	Le nombre de requêtes Web auxquelles des contrôles CAPTCHA ont été appliqués. Critères de notification : il existe une valeur différente de zéro. Une requête Web CAPTCHA correspond à une règle comportant un paramètre d'CAPTCHAaction. Cette métrique enregistre toutes les demandes qui correspondent, qu'elles comportent ou non un jeton CAPTCHA valide. Statistiques valides : somme

Métrique	Description
`RequestsWithValidCaptchaToken`	Le nombre de requêtes Web auxquelles des contrôles CAPTCHA étaient appliqués et pour lesquelles un jeton CAPTCHA était valide. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`CaptchasAttempted`	Le nombre de solutions soumises par un utilisateur final en réponse à un défi de type CAPTCHA. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`CaptchasSolved`	Le nombre de solutions de casse-tête CAPTCHA soumises qui ont résolu le casse-tête avec succès. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`ChallengeRequests`	Le nombre de requêtes Web auxquelles des contrôles de contestation ont été appliqués. Critères de notification : il existe une valeur différente de zéro. Une requête Web de défi correspond à une règle comportant un paramètre Challenge d'action. Cette métrique enregistre toutes les demandes qui correspondent, qu'elles comportent ou non un jeton de défi valide. Statistiques valides : somme

Métrique	Description
`RequestsWithValidChallengeToken`	Le nombre de requêtes Web auxquelles des contrôles de contestation étaient appliqués et pour lesquelles un jeton de défi était valide. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`PassedRequests`	Le nombre de demandes passées. Ceci n'est utilisé que pour les demandes soumises à une évaluation de groupe de règles sans correspondre à aucune des règles du groupe de règles. Critères de notification : il existe une valeur différente de zéro. Les demandes passées sont des demandes qui ne correspondent à aucune des règles du groupe de règles. Statistiques valides : somme

ACL Web, groupe de règles et dimensions de règles

Dimension	Description
`Region`	Obligatoire pour tous les types de ressources protégées, à l'exception CloudFront des distributions Amazon.
`Rule`	L’un des éléments suivants : • Nom de la métrique de la `Rule`. • ALL correspond à toutes les règles au sein d'un WebACL ou `RuleGroup` .

Dimension	Description
	• `Default_Action` (uniquement lorsqu'elle est combinée à la `WebACL` dimension), qui représent e l'action assignée à toute demande dont l'évaluat ion n'a pas été interrompue par l'action d'une règle dans l'ACL Web.
`RuleGroup`	Nom de la métrique de la `RuleGroup` .
`WebACL`	Nom de la métrique de la `WebACL`.
`Country`	Le pays d'origine de la demande. Il s'agit de la désignation à deux caractères de la norme 3166 de l'Organisation internationale de normalisation (ISO). Par exemple, États-Unis pour les États-Unis et UA pour l'Ukraine. Si une demande possède un `X-Forwarded-For` en-tête, AWS WAF utilisez-le pour déterminer ce paramètre. Dans le cas contraire, AWS WAF utilise le pays de l'adresse IP du client. Cette détermination est indépendante de toute logique que vous utilisez dans vos règles pour déterminer le pays d'origine. AWS WAF détermine l'emplacement des adresses IP à l'aide de bases de MaxMind données GeoIP.

Dimension	Description
`Attack`	Type d'attaque AWS WAF identifié dans la demande, en fonction des règles et des groupes de règles que vous utilisez dans votre ACL Web. Vos règles et celles des groupes de règles AWS gérés de base peuvent identifier les types d'attaque s. Par exemple, les correspondances de règles de script intersite (XSS) identifient les types d'attaque s XSS, tandis que les règles basées sur le taux identifient les types d'attaques volumétriques. Le type d'attaque indique généralement le type de règle qui a mis fin à l'évaluation de la demande Web.
`Device`	Type d'appareil du client qui a envoyé la demande, obtenu à partir de l'`user-agent` en-tête de la demande Web.
`ManagedRuleGroup`	Nom de la métrique de la `ManagedRuleGroup` .
`ManagedRuleGroupRule`	La règle contenue dans `ManagedRuleGroup` ce qui a été mise en correspondance.

Métriques et dimensions des étiquettes

Mesures relatives aux étiquettes ajoutées aux demandes lors de l'évaluation par vos règles et par les groupes de règles gérés que vous utilisez dans votre ACL Web. Pour plus d'informations, veuillez consulter Étiquettes sur les requêtes Web.

Pour chaque requête Web, AWS WAF stocke les statistiques d'au plus 100 étiquettes. Votre évaluation ACL Web peut appliquer plus de 100 étiquettes et établir une correspondance avec plus de 100 étiquettes, mais seules les 100 premières sont prises en compte dans les métriques.

Métriques relatives aux étiquettes

Métrique	Description
`AllowedRequests`	Nombre d'étiquettes sur les requêtes Web auxquelles le paramètre d'action était Allow appliqué. Les étiquettes peuvent avoir été ajoutées à tout moment pendant l'évaluation de la demande Web. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`BlockedRequests`	Nombre d'étiquettes sur les requêtes Web auxquelles le paramètre d'action était Block appliqué. Les étiquettes peuvent avoir été ajoutées à tout moment pendant l'évaluation de la demande Web. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`CountedRequests`	Nombre d'étiquettes ajoutées aux requêtes Web par des règles de groupe de règles comportant un paramètre Count d'action. Cette métrique n'est disponible que pour le propriétaire d'un groupe de règles, pour les règles internes au groupe de règles. Dans les autres cas, les métriques de l'étiquette de comptage sont intégrées à l'action de fin qui a été appliquée à la demande, comme Allow ouBlock. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme

Métrique	Description
`CaptchaRequests`	Le nombre d'étiquettes figurant sur les requêtes Web auxquelles une CAPTCHA action de résiliation a été appliquée. Les étiquettes peuvent avoir été ajoutées à tout moment pendant l'évaluation de la demande Web. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`ChallengeRequests`	Le nombre d'étiquettes figurant sur les requêtes Web auxquelles une Challenge action de résiliation a été appliquée. Les étiquettes peuvent avoir été ajoutées à tout moment pendant l'évaluation de la demande Web. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`AllowRuleMatch`	Le nombre de règles correspondantes qui ont à la fois généré l'étiquette associée et mis fin à l'évaluat ion de la demande par une Allow action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme

Métrique	Description
`BlockRuleMatch`	Le nombre de règles correspondantes qui ont à la fois généré l'étiquette associée et mis fin à l'évaluation de la demande par une Block action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`CountRuleMatch`	Le nombre de règles correspondantes qui ont à la fois généré l'étiquette associée et appliqué une Count action. Une demande peut générer plusieurs instances de cette métrique, si plusieurs règles sont configurées avec la même étiquette et la même action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`CaptchaRuleMatch`	Le nombre de règles correspondantes qui ont à la fois généré l'étiquette associée et mis fin à l'évaluation de la demande par une CAPTCHA action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme

Métrique	Description
`ChallengeRuleMatch`	Le nombre de règles correspondantes qui ont à la fois généré l'étiquette associée et mis fin à l'évaluation de la demande par une Challenge action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`CaptchaRuleMatchWithValidToken`	Le nombre de règles correspondantes qui ont à la fois généré l'étiquette associée et appliqué une action sans interruption. CAPTCHA Une demande peut générer plusieurs instances de cette métrique, si plusieurs règles sont configurées avec la même étiquette et la même action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`ChallengeRuleMatchWithValidToken`	Le nombre de règles correspondantes qui ont à la fois généré l'étiquette associée et appliqué une action sans interruption. Challenge Une demande peut générer plusieurs instances de cette métrique, si plusieurs règles sont configurées avec la même étiquette et la même action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme

Dimensions de l'étiquette

Dimension	Description
`Region`	Obligatoire pour tous les types de ressources protégées, à l'exception CloudFront des distributions Amazon.
`WebACL`	Nom de la métrique de la `WebACL`.
`RuleGroup`	Nom de la métrique de la `RuleGroup` . Utilisé pour la métrique`CountedRequests` .
`LabelNamespace`	Le préfixe d'espace de noms de l'étiquette ajoutée à la demande.
`Label`	Le nom de l'étiquette qui a été ajoutée à la demande.
`Context`	Le groupe de règles géré qui a servi de contexte à l'ajout d'étiquettes. Par exemple, le contexte des étiquettes de gestion des jetons `awswaf:managed:token:accepted` est le groupe de règles AWS WAF géré qui utilise la gestion des jetons sur la demande, tel que le groupe de règles géré par Bot Control ou ATP. Cette dimension ne s'applique pas à toutes les étiquettes.

Mesures et dimensions de visibilité des bots gratuites

Lorsque vous n'utilisez pas Bot Control dans votre ACL Web, AWS WAF applique le groupe de règles géré par Bot Control à un échantillon de vos requêtes Web, sans frais supplémentaires. Cela peut vous donner une idée du trafic de bots qui arrive sur vos ressources protégées. Pour plus d'informations sur le contrôle des robots, consultezAWS WAF Groupe de règles Bot Control.

Mesures de visibilité gratuites des bots

Métrique	Description
`SampleAllowedRequest`	Le nombre de demandes échantillonnées qui ont fait l'objet Allow d'une action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`SampleBlockedRequest`	Le nombre de demandes échantillonnées qui ont fait l'objet Block d'une action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`SampleCaptchaRequest`	Le nombre de demandes échantillonnées qui ont fait l'objet CAPTCHA d'une action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`SampleChallengeRequest`	Le nombre de demandes échantillonnées qui ont fait l'objet Challenge d'une action. Critères de notification : il existe une valeur différente de zéro. Statistiques valides : somme
`SampleCountRequest`	Le nombre de demandes échantillonnées qui ont fait l'objet Count d'une action. Critères de notification : il existe une valeur différente de zéro.

Métrique	Description
	Statistiques valides : somme

Dimensions de visibilité gratuites des bots

Dimension	Description
`Region`	Obligatoire pour tous les types de ressources protégées, à l'exception CloudFront des distributions Amazon.
`WebACL`	Nom de la métrique de la `WebACL`.
`BotCategory`	Le nom de la catégorie de bot détectée, en fonction des libellés des requêtes Web.
`VerificationStatus`	Nom du statut de vérification du bot détecté, basé sur les étiquettes des requêtes Web.
`Signal`	Le nom des signaux de bot détectés, basé sur les étiquettes des requêtes Web.

AWS Shield Advanced métriques

Shield Advanced publie les indicateurs CloudWatch de détection et d'atténuation d'Amazon ainsi que les indicateurs relatifs aux principaux contributeurs pour toutes les ressources qu'il protège. Ces indicateurs améliorent votre capacité à surveiller vos ressources en permettant de créer et de configurer des CloudWatch tableaux de bord et des alarmes pour celles-ci.

La console Shield Advanced présente des résumés de nombreux indicateurs qu'elle enregistre. Pour plus d’informations, consultez Visibilité sur les événements DDoS.

Si vous activez l'atténuation automatique des attaques DDoS au niveau de la couche application pour une protection de la couche application,

Emplacements des rapports métriques

Shield Advanced publie des statistiques dans la région de l'est des États-Unis (Virginie du Nord), `us-east-1` pour les domaines suivants :

- Les services mondiaux Amazon CloudFront et Amazon Route 53.
- Groupes de protection. Pour plus d'informations sur les groupes de protection, consultezAWS Shield Advanced groupes de protection.

Pour les autres types de ressources, Shield Advanced fournit des statistiques dans la région de la ressource.

Calendrier des rapports métriques

Shield Advanced communique des métriques à Amazon CloudWatch sur une AWS ressource plus fréquemment lors d'événements DDoS que lorsqu'aucun événement n'est en cours. Shield Advanced fournit des statistiques une fois par minute pendant un événement, puis une fois juste après la fin de l'événement.

Tant qu'aucun événement n'est en cours, Shield Advanced fournit des statistiques une fois par jour, à l'heure assignée à la ressource. Ce rapport périodique maintient les métriques actives et disponibles pour une utilisation dans des CloudWatch alarmes et des tableaux de bord personnalisés.

Recommandations relatives aux alarmes

Nous vous recommandons de créer des alarmes pour vous avertir des circonstances nécessitant une attention particulière. Comme point de départ, vous pouvez créer une alarme pour chaque ressource protégée signalant lorsque la métrique `DDoSDetected` de détection est différente de zéro. Une valeur différente de zéro dans cette métrique ne signifie pas nécessairement qu'une attaque DDoS est en cours, mais nous vous recommandons d'examiner de plus près l'état de la ressource lorsque la métrique est dans cet état.

En cas d'afflux de demandes, nous vous recommandons de créer des alarmes pour les vérifications composites qui tiennent également compte de facteurs tels que l'état de santé des applications et le volume de demandes Web. Vous pouvez choisir de déclencher une alarme sur les trois autres indicateurs qui indiquent le volume de trafic pour différentes dimensions du vecteur d'attaque. En tenant compte de la capacité de votre application et en vous alertant lorsque le trafic approche des limites de votre application, vous pouvez créer un ensemble de règles qui vous avertissent selon vos besoins, sans trop de bruit indésirable.

Rubriques

Métriques de détection

Shield Advanced fournit les métriques et les dimensions de l'espace de `AWS/DDoSProtection` noms.

Métriques de détection

Métrique	Description
`DDoSDetected`	Indique si un événement DDoS est en cours pour un Amazon Resource Name (ARN) spécifique. Cette métrique a une valeur différente de zéro lors d'un événement.
`DDoSAttackBitsPerSecond`	Nombre d'octets observés au cours d'un événement DDoS pour un Amazon Resource Name (ARN) spécifique. Cette métrique n'est disponible que pour les événements DDoS liés au réseau et aux couches de transport (couches 3 et 4). Cette métrique a une valeur différente de zéro lors d'un événement. Unités : octets
`DDoSAttackPacketsPerSecond`	Nombre de paquets observés au cours d'un événement DDoS pour un Amazon Resource Name (ARN) spécifique. Cette métrique n'est disponible que pour les événements DDoS liés au réseau et aux couches de transport (couches 3 et 4).

Métrique	Description
	Cette métrique a une valeur différente de zéro lors d'un événement. Unités : paquets
DDoSAttackRequestsPerSecond	Nombre de demandes observées au cours d'un événement DDoS pour un Amazon Resource Name (ARN) spécifique. Cette métrique est disponible uniquement pour les événement s DDoS de couche 7. Cette métrique est présentée uniquement pour les événements de couche 7 les plus significatifs. Cette métrique a une valeur différente de zéro lors d'un événement. Unités : demandes

Shield Advanced publie la DDoSDetected métrique sans aucune autre dimension. Les autres mesures de détection incluent les AttackVector dimensions correspondant au type d'attaque, dans la liste suivante :

- ACKFlood
- ChargenReflection
- DNSReflection
- GenericUDPReflection
- MemcachedReflection
- MSSQLReflection
- NetBIOSReflection
- NTPReflection
- PortMapper
- RequestFlood
- RIPReflection

- `SNMPReflection`
- `SSDPReflection`
- `SYNFlood`
- `UDPFragment`
- `UDPTraffic`
- `UDPReflection`

Mesures d'atténuation

Shield Advanced fournit des métriques et des dimensions dans l'espace de `AWS/DDoSProtection` noms.

Mesures d'atténuation

Métrique	Description
`VolumePacketsPerSecond`	Nombre de paquets par seconde qui ont été abandonnés ou transmis par une mesure d'atténuation déployée en réponse à un événement détecté. Unités : Paquets

Dimensions d'atténuation

Dimension	Description
`ResourceArn`	Amazon Resource Name (ARN)
`MitigationAction`	Le résultat d'une atténuation appliquée. Les valeurs possibles sont `Pass` ou `Drop`.

Statistiques relatives aux principaux contributeurs

Shield Advanced fournit des métriques dans l'espace de `AWS/DDoSProtection` noms.

Statistiques relatives aux principaux contributeurs

Métrique	Description
`VolumePacketsPerSecond`	Le nombre de paquets par seconde pour un contributeur de premier plan. Unités : Paquets
`VolumeBitsPerSecond`	Le nombre de bits par seconde pour le meilleur contributeur. Unités : bits

Shield Advanced publie les statistiques des principaux contributeurs par combinaison de dimensions qui caractérisent les contributeurs à l'événement. Vous pouvez utiliser l'une des combinaisons de dimensions suivantes pour les indicateurs des principaux contributeurs :

- `ResourceArn`, `Protocol`
- `ResourceArn`, `Protocol`, `SourcePort`
- `ResourceArn`, `Protocol`, `DestinationPort`
- `ResourceArn`, `Protocol`, `SourceIp`
- `ResourceArn`, `Protocol`, `SourceAsn`
- `ResourceArn`, `TcpFlags`

Dimensions des principaux contributeurs

Dimension	Description
`ResourceArn`	Nom de la ressource Amazon (ARN).
`Protocol`	Nom du protocole IP, `TCP` soit`UDP`.
`SourcePort`	Port TCP ou UDP source.
`DestinationPort`	Port TCP ou UDP de destination.
`SourceIp`	Adresse IP source.

Dimension	Description
`SourceAsn`	Numéro de système autonome source (ASN).
`TcpFlags`	Combinaison d'indicateurs présents dans un paquet TCP, séparés par un tiret (`-`). Les drapeaux surveillés sont `ACK`,`FIN`,`RST`,`SYN`. Cette valeur de dimension apparaît toujours triée par ordre alphabétique. Par exemple, `ACK-FIN-RST-SYN` , `ACK-SYN` et `FIN-RST`.

AWS Firewall Manager notifications

AWS Firewall Manager n'enregistre pas de statistiques, vous ne pouvez donc pas créer d' CloudWatch alarmes Amazon spécifiquement pour Firewall Manager. Cependant, vous pouvez configurer les notifications Amazon SNS pour vous avertir d'attaques potentielles. Pour créer des notifications Amazon SNS dans Firewall Manager, consultez. Étape 4 : configurer les notifications Amazon SNS et les alarmes Amazon CloudWatch

Journalisation des appels d'API AWS CloudTrail avec

AWS WAF AWS Shield Advanced, et AWS Firewall Manager sont intégrés à AWS CloudTrail, un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service. CloudTrail capture un sous-ensemble d'appels d'API pour ces services sous forme d'événements, y compris les appels depuis les AWS WAF consoles Shield Advanced ou Firewall Manager et depuis les appels de code vers les AWS WAF API Shield Advanced ou Firewall Manager. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, notamment des événements pour AWS WAF Shield Advanced ou Firewall Manager. Si vous ne configurez pas de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à ces services, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires.

Pour en savoir plus CloudTrail, notamment comment le configurer et l'activer, consultez le guide de AWS CloudTrail l'utilisateur.

CloudTrail est activé sur votre compte Compte AWS lorsque vous créez le compte. Lorsqu'une activité événementielle prise en charge se produit dans AWS WAF Shield Advanced ou Firewall Manager, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre Compte AWS. Pour plus d'informations, consultez la section Affichage des événements avec l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre navigateur Compte AWS, y compris ceux relatifs AWS WAFà Shield Advanced ou Firewall Manager, créez une trace. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions. Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d’informations, consultez les ressources suivantes :

- Présentation de la création d’un journal d’activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

AWS WAF informations dans AWS CloudTrail

Toutes les AWS WAF actions sont enregistrées AWS CloudTrail et documentées dans la référence de l'AWS WAF API. Par exemple, les appels à `ListWebACL`, `UpdateWebACL`, et la `DeleteWebACL` génération d'entrées dans les fichiers CloudTrail journaux.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l’identité permettent de déterminer les éléments suivants :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été faite par un autre AWS service

Pour plus d'informations, consultez CloudTrailUserIdentity Element.

Exemple : entrées de fichier AWS WAF journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. AWS CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et comprend des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Voici des exemples d'entrées de CloudTrail journal pour les opérations ACL AWS WAF Web.

Exemple : entrée de CloudTrail journal pour `CreateWebACL`


```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T03:43:07Z"
      }
    }
  },
  "eventTime": "2019-11-06T03:44:21Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "CreateWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
```

```
 "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
 "requestParameters": {
   "name": "foo",
   "scope": "CLOUDFRONT",
   "defaultAction": {
     "block": {}
   },
   "description": "foo",
   "rules": [
     {
       "name": "foo",
       "priority": 1,
       "statement": {
         "geoMatchStatement": {
           "countryCodes": [
             "AF",
             "AF"
           ]
         }
       },
       "action": {
         "block": {}
       },
       "visibilityConfig": {
         "sampledRequestsEnabled": true,
         "cloudWatchMetricsEnabled": true,
         "metricName": "foo"
       }
     }
   ],
   "visibilityConfig": {
     "sampledRequestsEnabled": true,
     "cloudWatchMetricsEnabled": true,
     "metricName": "foo"
   }
 },
 "responseElements": {
   "summary": {
     "name": "foo",
     "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
     "description": "foo",
     "lockToken": "67551e73-49d8-4363-be48-244deea72ea9",
```

```
      "aRN": "arn:aws:wafv2:us-east-1:112233445566:global/webacl/foo/
ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b"
    }
  },
  "requestID": "c51521ba-3911-45ca-ba77-43aba50471ca",
  "eventID": "afd1a60a-7d84-417f-bc9c-7116cf029065",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Exemple : entrée de CloudTrail journal pour `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"
}
```

Exemple : entrée de CloudTrail journal pour `UpdateWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:20:56Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "UpdateWebACL",
  "awsRegion": ""us-east-1,
```

```
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "defaultAction": {
      "block": {}
    },
    "description": "foo",
    "rules": [
      {
        "name": "foo",
        "priority": 1,
        "statement": {
          "geoMatchStatement": {
            "countryCodes": [
              "AF"
            ]
          }
        },
        "action": {
          "block": {}
        },
        "visibilityConfig": {
          "sampledRequestsEnabled": true,
          "cloudWatchMetricsEnabled": true,
          "metricName": "foo"
        }
      }
    ],
    "visibilityConfig": {
      "sampledRequestsEnabled": true,
      "cloudWatchMetricsEnabled": true,
      "metricName": "foo"
    },
    "lockToken": "67551e73-49d8-4363-be48-244deea72ea9"
  },
  "responseElements": {
    "nextLockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
  "requestID": "41c96e12-9790-46ab-b145-a230f358f2c2",
  "eventID": "517a10e6-4ca9-4828-af90-a5cff9756594",
```

```
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Exemple : entrée de CloudTrail journal pour `DeleteWebACL`

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "principalId",
    "arn": "arn:aws:sts::112233445566:assumed-role/Admin/session-name",
    "accountId": "112233445566",
    "accessKeyId": "accessKeyId",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "principalId",
        "arn": "arn:aws:iam::112233445566:role/Admin",
        "accountId": "112233445566",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2019-11-06T19:17:20Z"
      }
    }
  },
  "eventTime": "2019-11-06T19:25:17Z",
  "eventSource": "wafv2.amazonaws.com",
  "eventName": "DeleteWebACL",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "10.0.0.1",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/78.0.3904.87 Safari/537.36",
  "requestParameters": {
    "name": "foo",
    "scope": "CLOUDFRONT",
    "id": "ebbcb976-8d59-4d20-8ca8-4ab2f6b7c07b",
    "lockToken": "a6b54c01-7975-4e6d-b7d0-2653cb6e231d"
  },
```

```
  "responseElements": null,
  "requestID": "71703f89-e139-440c-96d4-9c77f4cd7565",
  "eventID": "2f976624-b6a5-4a09-a8d0-aa3e9f4e5187",
  "eventType": "AwsApiCall",
  "apiVersion": "2019-04-23",
  "recipientAccountId": "112233445566"
}
```

Exemple : entrées de fichier journal AWS WAF classiques

AWS WAF Classic est la version précédente de AWS WAF. Pour plus d'informations, veuillez consulter AWS WAF classique.

L'entrée de journal illustre les opérations `CreateRule`, `GetRule`, `UpdateRule` et `DeleteRule` :

```
{
  "Records": [
   {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:14Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "CreateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "name": "0923ab32-7229-49f0-a0e3-66c81example",
        "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample",
        "metricName": "0923ab32722949f0a0e366c81example"
      },
      "responseElements": {
        "rule": {
          "metricName": "0923ab32722949f0a0e366c81example",
          "ruleId": "12132e64-6750-4725-b714-e7544example",
          "predicates": [
```

```
        ],
        "name": "0923ab32-7229-49f0-a0e3-66c81example"
      },
      "changeToken": "l9434322-8685-4ed2-9c5b-9410bexample"
    },
    "requestID": "4e6b66f9-d548-11e3-a8a9-73e33example",
    "eventID": "923f4321-d378-4619-9b72-4605bexample",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-08-24",
    "recipientAccountId": "777777777777"
  },
  {
    "eventVersion": "1.03",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAIEP4IT4TPDEXAMPLE",
      "arn": "arn:aws:iam::777777777777:user/nate",
      "accountId": "777777777777",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "nate"
    },
    "eventTime": "2016-04-25T21:35:22Z",
    "eventSource": "waf.amazonaws.com",
    "eventName": "GetRule",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
      "ruleId": "723c2943-82dc-4bc1-a29b-c7d73example"
    },
    "responseElements": null,
    "requestID": "8e4f3211-d548-11e3-a8a9-73e33example",
    "eventID": "an236542-d1f9-4639-bb3d-8d2bbexample",
    "eventType": "AwsApiCall",
    "apiVersion": "2015-08-24",
    "recipientAccountId": "777777777777"
  },
  {
    "eventVersion": "1.03",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAIEP4IT4TPDEXAMPLE",
      "arn": "arn:aws:iam::777777777777:user/nate",
```

```
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:13Z",
      "eventSource": "waf.amazonaws.com",
      "eventName": "UpdateRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "ruleId": "7237b123-7903-4d9e-8176-9d71dexample",
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example",
        "updates": [
          {
            "predicate": {
              "type": "SizeConstraint",
              "dataId": "9239c032-bbbe-4b80-909b-782c0example",
              "negated": false
            },
            "action": "INSERT"
          }
        ]
      },
      "responseElements": {
        "changeToken": "32343a11-35e2-4dab-81d8-6d408example"
      },
      "requestID": "11918283-0b2d-11e6-9ccc-f9921example",
      "eventID": "00032abc-5bce-4237-a8ee-5f1a9example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    },
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAIEP4IT4TPDEXAMPLE",
        "arn": "arn:aws:iam::777777777777:user/nate",
        "accountId": "777777777777",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "nate"
      },
      "eventTime": "2016-04-25T21:35:28Z",
```

```
      "eventSource": "waf.amazonaws.com",
      "eventName": "DeleteRule",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "AWS Internal",
      "userAgent": "console.amazonaws.com",
      "requestParameters": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example",
        "ruleId": "3e3e2d11-fd8b-4333-8b03-1da95example"
      },
      "responseElements": {
        "changeToken": "fd232003-62de-4ea3-853d-52932example"
      },
      "requestID": "b23458a1-0b2d-11e6-9ccc-f9928example",
      "eventID": "a3236565-1a1a-4475-978e-81c12example",
      "eventType": "AwsApiCall",
      "apiVersion": "2015-08-24",
      "recipientAccountId": "777777777777"
    }
  ]
}
```


AWS Shield Advanced informations dans CloudTrail

AWS Shield Advanced prend en charge la journalisation des actions suivantes sous forme d'événements dans les fichiers CloudTrail journaux :

- ListAttacks
- DescribeAttack
- CreateProtection
- DescribeProtection
- DeleteProtection
- ListProtections
- CreateSubscription
- DescribeSubscription
- GetSubscriptionState

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root
- Si la demande a été effectuée avec les informations d’identification de sécurité temporaires d’un rôle ou d’un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Exemple : entrées du fichier journal Shield Advanced

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre les `ListProtections` actions `DeleteProtection` et.


```
[
 {
   "eventVersion": "1.05",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "123456789098765432123 1",
     "arn": "arn:aws:iam::123456789012:user/SampleUser",
     "accountId": "123456789012",
     "accessKeyId": "1AFGDT647FHU83JHFI81H",
     "userName": "SampleUser"
   },
   "eventTime": "2018-01-10T21:31:14Z",
   "eventSource": "shield.amazonaws.com",
   "eventName": "DeleteProtection",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "AWS Internal",
   "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
   "requestParameters": {
     "protectionId": "12345678-5104-46eb-bd03-agh4j8rh3b6n"
```

```
    },
    "responseElements": null,
    "requestID": "95bc0042-f64d-11e7-abd1-1babdc7aa857",
    "eventID": "85263bf4-17h4-43bb-b405-fh84jhd8urhg",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  },
  {
    "eventVersion": "1.05",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "123456789098765432123",
      "arn": "arn:aws:iam::123456789012:user/SampleUser",
      "accountId": "123456789012",
      "accessKeyId": "1AFGDT647FHU83JHFI81H",
      "userName": "SampleUser"
    },
    "eventTime": "2018-01-10T21:30:03Z",
    "eventSource": "shield.amazonaws.com",
    "eventName": "ListProtections",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "AWS Internal",
    "userAgent": "aws-cli/1.14.10 Python/3.6.4 Darwin/16.7.0 botocore/1.8.14",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "6accca40-f64d-11e7-abd1-1bjfi8urhj47",
    "eventID": "ac0570bd-8dbc-41ac-a2c2-987j90j3h78f",
    "eventType": "AwsApiCall",
    "apiVersion": "AWSShield_20160616",
    "recipientAccountId": "123456789012"
  }
]
```


AWS Firewall Manager informations dans CloudTrail

AWS Firewall Manager prend en charge l'enregistrement des actions suivantes sous forme d'événements dans les fichiers CloudTrail journaux :

- AssociateAdminAccount
- DeleteNotificationChannel
- DeletePolicy

- DisassociateAdminAccount
- PutNotificationChannel
- PutPolicy
- GetAdminAccount
- GetComplianceDetail
- GetNotificationChannel
- GetPolicy
- ListComplianceStatus
- ListPolicies

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été faite avec les informations d'identification de l'utilisateur root
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour plus d'informations, consultez l'élément CloudTrail UserIdentity.

Exemple : entrées du fichier journal de Firewall Manager

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre l'action `GetAdminAccount --`**>**.

```
{
                "eventVersion": "1.05",
```

```
                "userIdentity": {
                                "type": "AssumedRole",
                                "principalId": "123456789098765432123",
                                "arn": "arn:aws:sts::123456789012:assumed-role/Admin/
SampleUser",
                                "accountId": "123456789012",
                                "accessKeyId": "1AFGDT647FHU83JHFI81H",
                                "sessionContext": {
                                                "attributes": {
                                                                "mfaAuthenticated":
 "false",
                                                                "creationDate":
 "2018-04-14T02:51:50Z"
                                                               },
                                                "sessionIssuer": {
                                                                "type": "Role",
                                                                "principalId":
 "123456789098765432123",
                                                                "arn":
 "arn:aws:iam::123456789012:role/Admin",
                                                                "accountId":
 "123456789012",
                                                                "userName": "Admin"
                                                                 }
                                                  }
                                },
                "eventTime": "2018-04-14T03:12:35Z",
                "eventSource": "fms.amazonaws.com",
                "eventName": "GetAdminAccount",
                "awsRegion": "us-east-1",
                "sourceIPAddress": "72.21.198.65",
                "userAgent": "console.amazonaws.com",
                "requestParameters": null,
                "responseElements": null,
                "requestID": "ae244f41-3f91-11e8-787b-dfaafef95fc1",
                "eventID": "5769af1e-14b1-4bd1-ba75-f023981d0a4a",
                "eventType": "AwsApiCall",
                "apiVersion": "2018-01-01",
                "recipientAccountId": "123456789012"
    }
```

Utilisation de l' AWS Shield Advanced API AWS WAF and

Cette section explique comment envoyer des requêtes à l'API AWS WAF and Shield Advanced pour créer et gérer des ensembles de matchs, des règles et des ACL Web, AWS WAF ainsi que votre abonnement et vos protections dans Shield Advanced. Cette section vous permettra de vous familiariser avec les composants d'une requête, le contenu des réponses et l'authentification des requêtes.

Rubriques

Utilisation des AWS SDK

Si vous utilisez un langage qui AWS fournit un SDK pour, utilisez le SDK plutôt que d'essayer de vous frayer un chemin dans les API. Les SDK simplifient l'authentification, s'intègrent facilement à votre environnement de développement et fournissent un accès facile aux commandes Shield Advanced AWS WAF et à celles-ci. Pour plus d'informations sur AWS les SDK, consultez Télécharger les outils la rubriqueConfiguration de votre compte pour utiliser les services.

Envoyer des requêtes HTTPS à AWS WAF Shield Advanced

AWS WAF et les requêtes Shield Advanced sont des requêtes HTTPS, telles que définies par la RFC 2616. Comme toute requête HTTP, une requête adressée à AWS WAF ou à Shield Advanced contient une méthode de requête, un URI, des en-têtes de requête et un corps de requête. La réponse contient un code de statut HTTP, des en-têtes de réponse et parfois un corps de réponse.

URI de demande

L'URI de requête est toujours une seule barre oblique, `/`.

En-têtes HTTP

AWS WAF et Shield Advanced nécessitent les informations suivantes dans l'en-tête d'une requête HTTP :

Hôte (obligatoire)

Le point de terminaison qui spécifie où vos ressources sont créées. Pour plus d'informations sur les points de terminaison, consultez la section Points de terminaison AWS de service. Par exemple, la valeur de l'`Host`en-tête AWS WAF d'une CloudFront distribution est`waf.amazonaws.com:443`.

x-amz-date ou date (obligatoire)

La date utilisée pour créer la signature contenue dans l'en-tête `Authorization`. Spécifiez la date au format standard ISO 8601, avec l'heure UTC, comme illustré dans l'exemple suivant :

```
x-amz-date: 20151007T174952Z
```

Vous devez inclure soit `x-amz-date` ou `Date`. (Certaines bibliothèques client HTTP ne vous permettent pas de définir l'en-tête `Date`). Lorsqu'un `x-amz-date` en-tête est présent, AWS WAF ignore tout `Date` en-tête lors de l'authentification de la demande.

L'horodatage doit se situer dans les 15 minutes suivant l'heure du AWS système lorsque la demande est reçue. Si ce n'est pas le cas, la requête échoue avec le code d'erreur `RequestExpired` pour empêcher quelqu'un d'autre de relire vos requêtes.

Autorisation (requise)

Les informations requises pour l'authentification de la demande. Pour plus d'informations sur la construction de cet en-tête, consultez Authentification des requêtes.

X-Amz-Target (Obligatoire)

Une concaténation de `AWSWAF_` ou de `AWSShield_`, la version de l'API sans ponctuation, un point (`.`) et le nom de l'opération, par exemple :

`AWSWAF_20150824.CreateWebACL`

Content-Type (Conditional)

Spécifie que le type de contenu est JSON, ainsi que la version de JSON, comme illustré dans l'exemple suivant :

```
Content-Type: application/x-amz-json-1.1
```

État : obligatoire pour les POST demandes.

Content-Length (Conditional)

Longueur du message (sans les en-têtes) selon la RFC 2616.

Condition : obligatoire si le corps de la demande lui-même contient des informations (la plupart des boîtes à outils ajoutent automatiquement cet en-tête).

Voici un exemple d'en-tête de demande HTTP pour créer une liste ACL web dans 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
```

Corps de la demande HTTP

De nombreuses actions AWS WAF de l'API Shield Advanced nécessitent que vous incluiez des données au format JSON dans le corps de la demande.

L'exemple de demande suivant utilise une simple instruction JSON pour mettre à jour et inclure l'adresse IP 192.0.2.44 (représentée en notation CIDR sous la forme 192.0.2.44/32) : 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"
         }
      }
   ]
}
```

Réponses HTTP

Toutes les actions de l'API AWS WAF et Shield Advanced incluent des données au format JSON dans la réponse.

Voici quelques en-têtes importants dans la réponse HTTP et la façon dont vous devez les gérer dans votre application, le cas échéant :

HTTP/1.1

Cet en-tête est suivi d'un code d'état. Le code d'état 200 indique une opération réussie.

Type : chaîne

x-amzn- RequestId

Une valeur créée par AWS WAF ou Shield Advanced qui identifie de manière unique votre demande, par exemple,`K2QH8DN0U907N97FNA2GDLL80BVV4KQNSO5AEMVJF66Q9ASUAAJG`. Si vous rencontrez un problème avec AWS WAF, vous AWS pouvez utiliser cette valeur pour résoudre le problème.

Type : chaîne

Content-Length

Longueur du corps de la réponse en octets.

Type : chaîne

Date

Date et heure auxquelles AWS WAF ou Shield Advanced a répondu, par exemple, mercredi 07 octobre 2015 12:00:00 GMT.

Type : chaîne

Réponses d'erreur

Si une requête génère une erreur, la réponse HTTP contient les valeurs suivantes :

- un document d'erreur JSON comme corps de la réponse ;
- Content-Type
- un code de statut HTTP 3xx, 4xx ou 5xx applicable.

Voici un exemple de document d'erreur JSON :

```
HTTP/1.1 400 Bad Request
x-amzn-RequestId: b0e91dc8-3807-11e2-83c6-5912bf8ad066
x-amzn-ErrorType: ValidationException
Content-Type: application/json
Content-Length: 125
Date: Mon, 26 Nov 2012 20:27:25 GMT

{"message":"1 validation error detected: Value null at 'TargetString' failed to satisfy
 constraint: Member must not be null"}
```

Authentification des requêtes

Si vous utilisez un langage qui AWS fournit un SDK pour, nous vous recommandons d'utiliser le SDK. Tous les AWS SDK simplifient considérablement le processus de signature des demandes et vous font gagner un temps considérable par rapport à l'utilisation de l' AWS WAF API Shield

Advanced. De plus, les kits de développement logiciel s'intègrent facilement à votre environnement de développement et permettent de facilement accéder aux commandes associées.

AWS WAF et Shield Advanced exigent que vous authentifiiez chaque demande que vous envoyez en signant la demande. Pour signer une demande, vous calculez une signature numérique à l'aide d'une fonction de hachage cryptographique, qui renvoie une valeur de hachage basée sur l'entrée. L'entrée contient le texte de votre demande et votre clé d'accès secrète. La fonction de hachage renvoie une valeur de hachage que vous incluez dans la demande comme votre signature. La signature fait partie de l'en-tête `Authorization` de votre demande.

Après avoir reçu votre demande, AWS WAF Shield Advanced recalcule la signature en utilisant la même fonction de hachage et les mêmes entrées que celles que vous avez utilisées pour signer la demande. Si la signature obtenue correspond à celle de la demande, AWS WAF ou si Shield Advanced traite la demande. Si ce n'est pas le cas, la requête est rejetée.

AWS WAF et Shield Advanced prend en charge l'authentification à l'aide de AWS Signature Version 4. Le processus de calcul d'une signature peut être divisé en trois tâches :

Tâche 1 : créer une demande canonique

Créez votre demande HTTP au format canonique comme décrit dans Tâche 1 : créer une demande canonique pour Signature Version 4 du manuel Référence générale d'Amazon Web Services.

Tâche 2 : créer une chaîne de connexion

Créez une chaîne que vous utiliserez comme une des valeurs d'entrée pour votre fonction de hachage cryptographique. La chaîne, appelée la chaîne de connexion, est une concaténation des valeurs suivantes :

- Nom de l'algorithme de hachage
- Date de requête
- Chaîne d'informations d'identification
- Requête convertie sous forme canonique à partir de la tâche précédente

La chaîne d'informations d'identification elle-même est une concaténation de date, de région et d'informations de service.

Pour le paramètre `X-Amz-Credential`, spécifiez les éléments suivants :

- Le code pour le point de terminaison auquel vous envoyez la demande, `us-east-2`

- `waf` pour l'abréviation du service

Par exemple :

```
X-Amz-Credential=AKIAIOSFODNN7EXAMPLE/20130501/us-east-2/waf/
aws4_request
```

Tâche 3 : créer une signature

Créez une signature pour votre requête à l'aide d'une fonction de hachage de chiffrement qui accepte deux chaînes en entrée :

- Votre chaîne pour vous connecter, à partir de la tâche 2.
- Une clé dérivée. La clé dérivée est calculée en commençant par votre clé d'accès secrète et en utilisant la chaîne d'informations d'identification pour créer un ensemble de codes d'authentification de message basés sur le hachage (HMAC).

Informations connexes

Les ressources connexes suivantes peuvent s'avérer utiles lors de l'utilisation de ce service.

Les ressources suivantes sont disponibles pour AWS WAF AWS Shield Advanced, et AWS Firewall Manager.

- Directives de mise en œuvre AWS WAF — Publication technique contenant les recommandations actuelles pour la mise en œuvre AWS WAF afin de protéger les applications Web existantes et nouvelles.
- AWS forums de discussion — Un forum communautaire pour discuter de questions techniques liées à ce service et à d'autres AWS services.
- AWS WAF Forum de discussion — Un forum communautaire permettant aux développeurs de discuter de questions techniques liées à AWS WAF.
- Forum de discussion Shield Advanced : forum communautaire permettant aux développeurs de discuter de questions techniques liées à Shield Advanced.
- AWS WAF informations sur le produit : page Web principale contenant des informations AWS WAF, notamment sur les fonctionnalités, les prix, etc.
- Informations sur le produit Shield Advanced : page Web principale contenant des informations sur Shield Advanced, notamment sur les fonctionnalités, les prix, etc.

Les ressources suivantes sont disponibles pour Amazon Web Services.

- Cours et ateliers — Liens vers des cours spécialisés et basés sur des rôles, ainsi que des ateliers à votre rythme pour vous aider à perfectionner vos AWS compétences et à acquérir une expérience pratique.
- AWS Centre pour développeurs : découvrez les didacticiels, téléchargez des outils et découvrez les événements AWS destinés aux développeurs.
- AWS Outils de développement : liens vers des outils de développement, des SDK, des boîtes à outils IDE et des outils de ligne de commande pour le développement et la gestion AWS d'applications.
- Centre de ressources pour la mise en route : découvrez comment configurer votre application Compte AWS, rejoindre la AWS communauté et lancer votre première application.
- Tutoriels pratiques — Suivez les step-by-step didacticiels pour lancer votre première application sur AWS.

- AWS Livres blancs : liens vers une liste complète de livres AWS blancs techniques, traitant de sujets tels que l'architecture, la sécurité et l'économie, rédigés par des architectes de AWS solutions ou d'autres experts techniques.
- AWS Support Centre — Le centre de création et de gestion de vos AWS Support dossiers. Comprend également des liens vers d'autres ressources utiles, telles que des forums, des FAQ techniques, l'état de santé du service et AWS Trusted Advisor.
- AWS Support— La principale page Web contenant des informations sur AWS Support un one-on-one canal d'assistance à réponse rapide pour vous aider à créer et à exécuter des applications dans le cloud.
- Contactez-nous : point de contact central pour toute question relative à la facturation AWS , à votre compte, aux événements, à des abus ou à d'autres problèmes.
- AWS Conditions du site — Informations détaillées sur nos droits d'auteur et notre marque commerciale ; votre compte, votre licence et l'accès au site ; et d'autres sujets.

Historique du document

Cette page répertorie les modifications importantes apportées à cette documentation.

Les fonctionnalités du service sont parfois déployées progressivement AWS dans les régions où un service est disponible. Nous mettons à jour cette documentation pour la première version uniquement. Nous ne fournissons pas d'informations sur la disponibilité des régions et n'annonçons pas les déploiements régionaux ultérieurs. Pour plus d'informations sur la disponibilité des fonctionnalités du service dans les régions et pour vous abonner aux notifications concernant les mises à jour, voir Quelles sont les nouveautés AWS ? .

Modification	Description	Date
Clarifier le fonctionnement de l'analyse du corps JSON	Couverture mise à jour pour l'inspection du corps JSON afin de clarifier la manière dont l' AWS WAF analyse du corps est gérée et le comportement de repli de l'analyse du corps.	25 juin 2024
Règles AWS gérées mises à jour pour AWS WAF	Mise à jour de l'ensemble de règles du système d'exploit ation Linux.	6 juin 2024
AWS WAF modifications de politique gérées	Mis à jour `WAFV2Logg ingServiceRolePoli cy` et `AWSServic eRoleForWAFV2Loggi ng` pour ajouter des identifia nts de relevé (SID) aux paramètres des autorisations.	3 juin 2024
AWS WAF suivi géré des modifications des politiques	AWS WAF a commencé à suivre les modifications apportées à la politique gérée `WAFV2LoggingServic eRolePolicy` et au rôle	3 juin 2024

	lié au service. `AWSServiceRoleForWAFV2Logging`	
Règles AWS gérées mises à jour pour AWS WAF	Les groupes de règles gérés par Bot Control, ATP et ACFP sont désormais versionnés et fourniront des notifications SNS pour les mises à jour de version, comme les autres règles gérées versionnées AWS .	29 mai 2024
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles du système d'exploitation POSIX,`AWSManagedRulesUnixRuleSet` .	28 mai 2024
CAPTCHAet Challenge actions	Ajout d'une précision selon laquelle les clients du navigateur ont besoin du protocole HTTPS pour exécuter des puzzles CAPTCHA et des défis silencieux.	24 mai 2024
Intégration à Amazon Security Lake	Vous pouvez désormais utiliser Security Lake pour collecter des données de trafic ACL Web. Pour plus d'informations, consultez la section Collecte de données à partir AWS des services dans le guide de l'utilisateur d'Amazon Security Lake.	22 mai 2024

Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles de base (CRS).	21 mai 2024
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles de base de données SQLi.	14 mai 2024
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour mettre AWS WAF à jour les entrées erronées connues et les groupes de règles du système d'exploitation POSIX.	8 mai 2024
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour mettre AWS WAF à jour le groupe de règles du système d'exploitation Windows.	3 mai 2024
AWS WAF exemples de code Kotlin Android du SDK mobile	Ajout d'un exemple de code pour les intégrations Android basées sur Kotlin.	2 mai 2024
AWS WAF métriques, dimensions ajoutées et nouvelles métriques	AWS WAF ajout d'une nouvelle dimension pour `ManagedRuleSetRule` les métriques intégrées aux règles et de nouvelles métriques pour l'action de règle correspon dante pour les métriques d'étiquette.	2 mai 2024

AWS Firewall Manager prend en charge les politiques ACL du réseau	Firewall Manager prend désormais en charge la gestion des listes de contrôle d'accès réseau (ACL) Amazon VPC via les politiques ACL du réseau Firewall Manager.	25 avril 2024
AWS Firewall Manager mises à jour des politiques de sécurité	Mises à jour `FMSServiceRolePolicy` pour ajouter des autorisations pour la gestion des ACL réseau.	22 avril 2024
Liste des mesures de contrôle de santé mise à jour	Nous avons retiré certains indicateurs de la liste des indicateurs couramment utilisés dans les bilans de santé.	16 avril 2024
Mises à jour des politiques de groupe de sécurité de Firewall Manager	Nous avons mis à jour nos politiques de groupe de sécurité relatives aux audits d'utilisation et amélioré la documentation. Consultez la section sur la politique d'audit d'utilisation et les sections sur les meilleures pratiques et les limites.	2 avril 2024
Exemples de contrôle des bots mis à jour	Ajout d'exemples illustrant le niveau d'inspection ciblé et mise à jour des exemples existants pour refléter les meilleures pratiques.	27 mars 2024

Exemples ATP mis à jour	Ajout d'un exemple illustrant la configuration de l'inspection des réponses et mise à jour des exemples existants pour refléter les meilleures pratiques.	27 mars 2024
Exemples ACFP mis à jour	Ajout d'un exemple illustrant la configuration de l'inspection des réponses.	27 mars 2024
Mettre à jour les limites du flux de CloudWatch log Amazon Logs	AWS WAF n'impose plus de limites d'ACL par site Web pour la publication des journaux dans les flux de CloudWatch journaux.	27 mars 2024
AWS Shield Advanced protections de la couche d'application (couche 7)	Directives générales et de bonnes pratiques mises à jour pour la détection et l'atténuation de la couche d'application, l'utilisation des ACL Web, les règles basées sur le débit et l'atténuation automatique des attaques DDoS au niveau de la couche application.	14 mars 2024
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour mettre AWS WAF à jour le groupe de règles de réputation IP.	13 mars 2024
Modifications apportées aux limites de taille des corps inspectés	AWS WAF prend désormais en charge des limites de taille plus élevées pour les inspections corporelles pour certaines ressources régionales.	7 mars 2024

Fenêtre d'évaluation configurable pour les règles AWS WAF basées sur les taux	Vous pouvez désormais configurer la fenêtre temporelle utilisée par les règles basées sur les taux pour compter les demandes, à 1, 2, 5 ou 10 minutes. La valeur par défaut est 5, ce qui était la seule option avant cette version.	28 février 2024
Informations de journalisation étendues pour CAPTCHA et Challenge	Le niveau supérieur `captchaResponse` et `challengeResponse` les champs sont désormais renseignés avec la dernière de ces actions à appliquer à une demande, qu'elle soit terminante ou non. Auparavant, ces champs étaient remplis uniquement pour mettre fin aux actions.	22 février 2024
JavaScript Gestion des clés de l'API CAPTCHA	Vous pouvez désormais supprimer les clés d'API CAPTCHA JS via les AWS WAF API.	6 février 2024
AWS WAF Captcha Puzzles audio	La version audio du casse-tête CAPTCHA est désormais compatible avec plusieurs langues.	6 février 2024
AWS WAF étiquetage des défis et des jetons CAPTCHA	La gestion des jetons ajoute désormais des étiquettes pour le jeton CAPTCHA et a amélioré l'étiquetage des jetons pour le jeton de défi.	20 décembre 2023

Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour mettre AWS WAF à jour le groupe de règles relatives aux entrées erronées connues.	16 décembre 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour mettre AWS WAF à jour le groupe de règles relatives aux entrées erronées connues.	14 décembre 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles de base (CRS).	6 décembre 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : AWS WAF Bot Control.	5 décembre 2023
Configuration AWS Config requise pour Firewall Manager mise à jour	Si vous utilisez un rôle IAM personnalisé au lieu du rôle géré par Firewall Manager pour AWS Config, vous devez vous assurer que votre politique d'autorisation autorise l' AWS Config enregistreur à enregistrer les ressources de Firewall Manager.	17 novembre 2023
AWS WAF tableaux de bord de console	Nous avons corrigé les instructions relatives à l'affichage de toutes les règles et avons échantillonné des demandes d'ACL Web dans la AWS WAF console.	17 novembre 2023

Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles Bot Control.	14 novembre 2023
AWS WAF la console possède de nouveaux tableaux de bord ACL Web	La page ACL Web de la AWS WAF console contient de nouveaux tableaux de bord d'aperçu du trafic Web.	14 novembre 2023
Groupe de règles géré ATP mis à jour	Informations d'étiquette corrigées pour les règles `VolumetricIpFailedLoginResponseHigh` et `VolumetricSessionFailedLoginResponseHigh` .	13 novembre 2023
Groupe de règles géré par ACFP mis à jour	Informations d'étiquette corrigées pour les règles `VolumetricIPSuccessfulResponse` et `VolumetricSessionSuccessfulResponse` .	13 novembre 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles de base (CRS).	2 novembre 2023

Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative	Shield Advanced maintient désormais une règle basée sur le débit dans le groupe de règles d'atténuation automatique qui limite le volume de demandes provenant d'adresses IP connues pour être à l'origine d'attaques DDoS.	31 octobre 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles de base (CRS).	30 octobre 2023
Le groupe de règles géré par Bot Control a supprimé l'étiquette de signal pour la demande (CSP)	Le groupe de règles géré par Bot Control a supprimé l'étiquette de signal qui indique le fournisseur de services cloud (CSP).	28 octobre 2023
Étiquette de signal du groupe de règles géré par Bot Control pour la demande (CSP)	Les étiquettes de signaux du groupe de règles géré par Bot Control incluent une étiquette indiquant le fournisseur de services cloud (CSP).	27 octobre 2023
Informations sur les autorisations AWS WAF IAM mises à jour	Pour les AWS WAF actions qui gèrent les associations ACL Web, la section des actions de politique répertorie désormais les autorisations requises pour chaque type de ressource d'application Web.	25 octobre 2023

Firewall Manager : gestion des ACL Web modifiées	Lorsque vous activez la gestion des ACL Web non associées, Firewall Manager n'inclut pas les ACL Web modifiées dans le nettoyage ponctuel des ressources inutilisées.	19 octobre 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles du système d'exploitation POSIX,`AWSManagedRulesUnixRuleSet` .	12 octobre 2023
AWS WAF métriques, dimensions ajoutées	AWS WAF ajout de nouvelles dimensions pour l'affichage des métriques ACL Web.	12 octobre 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles de base (CRS).	11 octobre 2023
Mise à jour de la AWS WAF spécification du SDK mobile	L'`storeTokenInCookieStorage` opération a été ajoutée à`WAFTokenProvider` .	11 octobre 2023
Règles AWS gérées pour les déploiements exceptionnels pour AWS WAF	AWS Managed Rules for AWS WAF a publié deux versions statiques du groupe de règles relatives aux entrées erronées connues et a mis à jour la version par défaut pour qu'elle pointe vers la version statique la plus récente.	4 octobre 2023

AWS WAF Transformation de texte par décodage d'entités HTML	Les fonctionnalités de la transformation du texte par décodage d'entités HTML ont été étendues.	4 octobre 2023
Ajout d'une nouvelle option à la politique commune du groupe de sécurité Firewall Manager	Firewall Manager peut désormais distribuer des références de groupes de sécurité à des répliques de groupes de sécurité.	3 octobre 2023
AWS WAF ajoute l'inspection de l'empreinte digitale JA3	Vous pouvez désormais effectuer une correspondance exacte avec l'empreinte JA3 de la requête Web, pour les CloudFront distributions Amazon et les équilibreurs de charge d'application.	26 septembre 2023
Mises à jour des paramètres des règles de politique de groupe de sécurité de Firewall Manager	Firewall Manager prend désormais en charge le référencement des groupes de sécurité, des groupes de sécurité principaux aux groupes de sécurité répliqués.	25 septembre 2023
Mise à jour de l'atténuation automatique des attaques DDoS dans la couche d'application Shield Advanced	Firewall Manager prend désormais en charge les ressources Application Load Balancer pour les politiques Shield Advanced configurées avec une atténuation automatique des attaques DDoS au niveau de la couche application.	14 septembre 2023

Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : AWS WAF Bot Control.	6 septembre 2023
AWS WAF Contrôle des robots	Le niveau de protection ciblé du groupe de règles géré par Bot Control inspecte désormais la réutilisation des jetons entre les adresses IP. Il propose également désormais une analyse optionnelle par apprentissage automatique des statistiques de trafic afin de détecter certaines activités liées aux robots.	6 septembre 2023
Mise à jour de la AWS WAF spécification du SDK mobile	Les valeurs min, max et par défaut ont été abaissées, `tokenRefreshDelaySec` de 300 au maximum, et de 300 par défaut à 88, au maximum 300 et à 88 par défaut.	5 septembre 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles AWS WAF Bot Control.	30 août 2023
Shield Advanced : atténuation automatique des attaques DDoS au niveau de la couche applicative	Ajout de conseils d'utilisation AWS CloudFormation pour gérer les ACL Web que vous utilisez avec une atténuation automatique des attaques DDoS au niveau de la couche application.	30 août 2023

Nouvelle option de stratégie de groupe de sécurité pour l'audit du contenu de Firewall Manager	Ajout d'une nouvelle option pour auditer les groupes de règles trop permissifs et amélioration des descriptions des procédures de console.	29 août 2023
Nouveau Firewall Manager Shield et nouvelle option AWS WAF de politique	Si vous activez la gestion des ACL Web non associées dans and AWS WAF Shield, Firewall Manager ne crée des ACL Web dans les comptes relevant du champ d'applica tion de la politique que si les ACL Web sont utilisées par au moins une ressource.	9 août 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles de base (CRS).	26 juillet 2023
Agrégation de règles basée sur le taux sur le chemin de l'URI	Vous pouvez désormais spécifier le chemin de l'URI dans vos clés d'agrégation personnalisées pour les règles basées sur le taux.	19 juillet 2023
Nouvelle option AWS WAF de règle de politique dans AWS Firewall Manager	AWS Firewall Manager ajoute la prise en charge de la configuration des limites de taille d'inspection du corps des requêtes AWS WAF Web.	18 juillet 2023

AWS WAF modifications de politique gérées	Mis à jour `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , et `AWSWAFConsoleReadOnlyAccess` pour ajouter AWS un accès vérifié aux types de ressources avec lesquels vous pouvez vous protéger AWS WAF.	17 juin 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour AWS WAF ajouter le groupe de règles`AWSManagedRulesACFPRuleSet` .	13 juin 2023
Mise à jour de AWS WAF la prévention du piratage de comptes Fraud Control (ATP)	Vous pouvez désormais spécifier le point de terminaison de connexion pour le groupe de règles géré par ATP à l'aide d'une expression régulière.	13 juin 2023
Nouvelles informations pour l'API CAPTCHA JavaScript	Une nouvelle section décrit comment servir un casse-tête CAPTCHA personnalisé lorsque l'on AWS WAF répond à une demande contenant un CAPTCHA.	13 juin 2023

Nouveau groupe de règles géré par l'ACFP	Utilisez le nouveau groupe de règles `AWSManagedRulesACFPRuleSet` pour détecter et bloquer les tentatives de création de compte frauduleuses.	13 juin 2023
Création d'un nouveau compte AWS WAF Fraud Control, prévention de la fraude (ACFP)	Vous pouvez détecter et bloquer les tentatives de création de comptes frauduleuses grâce au nouveau groupe `AWSManagedRulesACFPRuleSet` de règles géré AWS WAF Fraud Control pour la création de comptes et la prévention de la fraude (ACFP). Avec les CloudFront distributions protégées, vous pouvez également utiliser l'ACFP pour bloquer les tentatives de création de nouveaux comptes de la part de clients ayant récemment soumis trop de tentatives de création de compte infructueuses.	13 juin 2023

AWS WAF modifications de politique gérées	Mis à jour `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , et `AWSWAFConsoleReadOnlyAccess` pour corriger les paramètres d'accès aux AWS App Runner services.	6 juin 2023
Limitation ajoutée pour les politiques de groupe de sécurité de Firewall Manager	Si un VPC partagé est ultérieurement départagé , Firewall Manager ne supprimera pas les groupes de sécurité répliqués dans le compte associé.	2 juin 2023
Nouveau composant AWS WAF de demande : Header order	Vous pouvez désormais comparer les noms des en-têtes de la demande à une liste ordonnée.	30 mai 2023
Règles AWS gérées mises à jour pour AWS WAF	Mise à jour de l'ensemble de règles du système d'exploitation Linux.	22 mai 2023
Mise à jour de l'organisation de la section AWS WAF des règles	Les listes d'instructions de règles sont désormais regroupées par type d'instruction.	16 mai 2023

Sujet déplacé : Liste des adresses IP dont le débit est limité	La rubrique relative à la liste des adresses IP dont le débit est limité par une règle basée sur le taux se trouve désormais dans la rubrique des règles basées sur le taux.	16 mai 2023
Options étendues pour les règles basées sur les taux	Vous pouvez désormais limiter le débit des requêtes Web en fonction de clés d'agrégation autres que les adresses IP, et vous pouvez les agréger à l'aide de combinaisons de clés. Vous pouvez également limiter le débit de toutes les demandes correspondant à une instruction scope-down, sans autre agrégation.	16 mai 2023
Le quota de Firewall Manager augmente	Le nombre de politique s Firewall Manager par organisation a été augmenté AWS Organizations de 20 à 50. Le nombre maximum de groupes de sécurité principau x par politique a été augmenté de un à trois. Le nombre maximum de WCU est passé d'un quota souple à un quota strict.	5 mai 2023

Augmentation du nombre maximum de WCU par groupe de règles	Vous pouvez désormais utiliser jusqu'à 5 000 unités de capacité ACL Web (WCU) par groupe de règles sans demander d'augmentation auprès du support. Cette nouvelle limite ne peut pas être augmentée.	1er mai 2023
AWS WAF Emplacements des compartiments de log Amazon S3 avec préfixes	AWS WAF autorise désormais les préfixes dans les noms des compartiments de log Amazon S3.	1er mai 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles de base (CRS).	28 avril 2023
Ajout de la prise en charge des instances d'accès AWS vérifié pour AWS WAF	Vous pouvez désormais associer une ACL AWS WAF Web à une instance d'accès vérifié. Cette modification n'est disponible que dans la dernière version de AWS WAF et non dans AWS WAF Classic.	28 avril 2023
Chapitre révisé sur le travail avec plusieurs administrateurs de Firewall Manager	Vous pouvez désormais désigner plusieurs administr ateurs Firewall Manager pour créer et gérer les ressources de pare-feu de votre entrepris e.	24 avril 2023
AWS Firewall Manager mise à jour des politiques gérée	Mis à jour `FMSServic eRolePolicy` .	21 avril 2023

Nouvelle intégration d'applications JavaScript clientes pour CAPTCHA	Vous pouvez désormais personnaliser le placement et les caractéristiques du puzzle CAPTCHA dans vos applications JavaScript clientes.	20 avril 2023
L'intégration des applications est rebaptisée intégration intelligente des menaces	Nous avons renommé la fonctionnalité existante pour les intégrations d'applications clientes en intégrations intelligentes des menaces, afin de faire la distinction entre cette fonctionnalité et la nouvelle intégration d'applications CAPTCHA pour. JavaScript	20 avril 2023
Tarification variable pour les WCU ACL Web au-delà de 1 500	L'utilisation de plus de 1 500 unités de capacité ACL Web (WCU) dans votre ACL Web entraîne des coûts supplémentaires, qui sont ajustés automatiquement à mesure que l'utilisation de votre WCU ACL Web augmente et diminue. Le nombre maximum d'ACL Web est de 5 000 WCU.	11 avril 2023
Augmentation du nombre maximum de WCU par ACL Web	Vous pouvez désormais utiliser jusqu'à 5 000 unités de capacité ACL Web (WCU) par ACL Web sans demander d'augmentation auprès du support. Cette nouvelle limite ne peut pas être augmentée.	11 avril 2023

Limites de taille d'inspection corporelle pour les CloudFront ACL Web	Pour les ACL Web qui protègent les CloudFront distributions Amazon, vous pouvez augmenter la limite de taille d'inspection corporell e jusqu'à 64 Ko dans votre configuration ACL Web.	11 avril 2023
Augmentation de la taille d'inspection de la carrosserie pour CloudFront	La taille maximale d'inspect ion AWS WAF corporelle pour les CloudFront distributions Amazon est augmentée de 8 Ko à 64 Ko. La limite de taille d'inspection par défaut CloudFront est de 16 Ko.	11 avril 2023
Nouvelles options AWS WAF de règles de politique dans AWS Firewall Manager	AWS Firewall Manager ajoute la prise en charge des groupes de règles ATP (AWS WAF Fraud Control Account Takeover Preventio n) et AWS WAF Bot Control AWS Managed Rules, des destinations de journalisation Amazon S3, des dérogatio ns aux actions des règles `CAPTCHA` et des actions de `Challenge` règles, ainsi que des listes de domaines à jetons.	7 avril 2023
Firewall Manager prend en charge les compartiments Amazon S3 comme destinati ons de journalisation pour la AWS WAF journalisation	Vous pouvez désormais utiliser les compartiments Amazon S3 comme destinati ons de journalisation dans vos AWS WAF politiques.	7 avril 2023

AWS WAF modifications de politique gérées	Mis à jour `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , et `AWSWAFConsoleReadOnlyAccess` pour ajouter AWS App Runner des services aux types de ressources que vous pouvez utiliser pour vous protéger AWS WAF.	30 mars 2023
Ajout d'un avertissement concernant l'utilisation de balises dans les politiques des groupes de sécurité	Firewall Manager ne met pas à jour les balises des groupes de sécurité existants et ne crée pas de nouveaux groupes de sécurité si la politique contient des balises en conflit avec la politique de balises de l'entreprise.	28 mars 2023
Mise à jour des informations relatives aux rôles de	Mise à jour de la procédure d'utilisation d'un rôle de service avec Firewall Manager.	8 mars 2023
Informations corrigées sur la manière dont les règles basées sur le débit permettent de limiter le débit	Les règles basées sur le taux avec instructions de portée réduite ne limitent que les demandes de limitation de débit qui correspondent à l'instruction de portée réduite de la règle. Nous indiquions que la limite s'appliquait à toutes les demandes d'adresse IP à débit limité.	1er mars 2023

Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles d'application PHP.	27 février 2023
Ajout de la prise en charge AWS App Runner de AWS WAF	Vous pouvez désormais associer une ACL AWS WAF Web à un AWS App Runner service. Cette modification n'est disponible que dans la dernière version de AWS WAF et non dans AWS WAF Classic.	23 février 2023
Mise à jour des directives IAM pour AWS Firewall Manager	Mise à jour du guide s'aligner sur les bonnes pratiques IAM. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM.	16 février 2023
Règles AWS gérées mises à jour pour AWS WAF	AWS Managed Rules for a AWS WAF mis à jour le groupe `AWSManagedRulesATPRuleSet` de règles afin d'ajouter l'inspection des réponses de connexion dans les ACL Web qui protègent les CloudFront distributions Amazon.	15 février 2023

AWS WAF Contrôle des fraudes (ATP), prévention du piratage de comptes, inspection de la réponse à la connexion	Pour les CloudFront distributions protégées, vous pouvez désormais utiliser ATP pour bloquer les nouvelles tentatives de connexion des clients ayant récemment soumis trop de tentatives de connexion infructueuses.	15 février 2023
Règles AWS gérées mises à jour pour AWS WAF	L'ensemble de règles de base a été mis à jour.	25 janvier 2023
Meilleures pratiques pour une atténuation intelligente des menaces	Ajout d'une section présentant les meilleures pratiques pour la mise en œuvre du contrôle des bots, de l'ATP et d'autres fonctionnalités intelligentes d'atténuation des menaces.	22 janvier 2023
Comment inspecter les pseudo-en-têtes HTTP/2	Ajout d'une section qui fait correspondre les pseudo-en-têtes HTTP/2 aux composants de requête Web correspondants.	20 janvier 2023
Mise à jour du guide IAM pour Classic AWS WAF	Mise à jour du guide s’aligner sur les bonnes pratiques IAM. Pour plus d’informations, consultez Bonnes pratiques de sécurité dans IAM.	3 janvier 2023
Mise à jour des directives IAM pour AWS WAF	Mise à jour du guide s’aligner sur les bonnes pratiques IAM. Pour plus d’informations, consultez Bonnes pratiques de sécurité dans IAM.	3 janvier 2023

Mise à jour des directives IAM pour AWS Shield	Mise à jour du guide s'aligner sur les bonnes pratiques IAM. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM.	3 janvier 2023
Mise à jour des politiques de pare-feu DNS d'Amazon Route 53 Resolver	Ajout d'informations sur la suppression des groupes de règles du pare-feu DNS Amazon Route 53 Resolver.	29 décembre 2022
Règles AWS gérées mises à jour pour AWS WAF	Mise à jour de l'ensemble de règles du système d'exploit ation Linux.	15 décembre 2022
Règles AWS gérées mises à jour pour AWS WAF	L'ensemble de règles de base a été mis à jour.	5 décembre 2022
Firewall Manager ajoute la prise en charge des politique s de Fortigate Cloud Native Firewall (CNF) as a Service	Firewall Manager prend désormais en charge les politiques Fortigate CNF.	2 décembre 2022
Suppression AWS Config de l'exigence relative aux politiques de pare-feu DNS	Pour les politiques de pare-feu DNS, il vous suffit désormais d'activer Config pour le type de ressource EC2 VPC.	17 novembre 2022
AWS Firewall Manager mise à jour des politiques gérée	Mis à jour `FMSServiceRolePolicy` .	15 novembre 2022

Extension des options linguistiques pour le puzzle AWS WAF CAPTCHA	Le casse-tête CAPTCHA propose désormais ses instructions écrites en plusieurs langues. Les instructions contenues dans chaque puzzle audio sont toujours fournies en anglais uniquement.	11 novembre 2022
Nouveaux quotas de Firewall Manager pour les ensembles de ressources	Ajout de nouveaux quotas pour les ensembles de ressources.	8 novembre 2022
Ajouter la prise en charge des ensembles de ressources	Vous pouvez créer des ensembles de ressources pour regrouper les ressources à gérer dans le cadre d'une politique Firewall Manager.	8 novembre 2022
Ajout de la prise en charge de l'importation de pare-feux depuis Network Firewall	Vous pouvez désormais importer et gérer les pare-feux existants dans les politiques de Network Firewall à l'aide d'ensembles de ressources.	8 novembre 2022
AWS Firewall Manager mise à jour des politiques gérée	Mis à jour `AWSFMAdminReadOnlyAccess` .	2 novembre 2022
La déclaration Geo Match ajoute désormais des étiquettes aux demandes relatives au pays et à la région	Vous pouvez désormais gérer les origines des demandes géographiques au niveau de la région en combinant la correspondance géographique et la correspondance des étiquettes.	31 octobre 2022

La section de niveau supérieur a été renommée : Protections gérées	La section s'intitule désormais Atténuation AWS WAF intelligente des menaces, conformément à nos pages marketing.	27 octobre 2022
Nouveau niveau de protection ciblée dans le groupe de règles gérées par Bot Control	Le groupe de règles géré par Bot Control propose désormais des règles supplémentaires ciblées pour la détection et l'atténuation des bots sophistiqués. Ce niveau de protection est disponible moyennant des frais supplémentaires.	27 octobre 2022
Nouvelle section sur les AWS WAF jetons	Découvrez comment les jetons sont AWS WAF utilisés pour atténuer les menaces de manière intelligente.	27 octobre 2022
Ajout d'une remarque importante concernant la mise à jour des politiques de Firewall Manager Network Firewall	Lorsque vous mettez à jour une politique de Firewall Manager, toutes les politiques de Network Firewall créées par cette politique sont mises à jour en fonction de la configuration de politique Network Firewall de la politique de Firewall Manager.	27 octobre 2022

Dérogations d'actions dans les groupes de règles	Vous pouvez désormais remplacer les actions des règles d'un groupe de règles par n'importe quel paramètre d'action des règles. Comme pour la dérogation Count d'action précédente, vous pouvez appliquer vos dérogations à toutes les règles d'un groupe de règles et à des règles individuelles.	27 octobre 2022
AWS WAF nouvelle option d'action de Challenge règle	Vous pouvez configurer des règles pour utiliser aChalleng e, afin de vérifier que les demandes sont envoyées par les navigateurs.	27 octobre 2022
AWS WAF permet le partage de jetons entre plusieurs applications protégées	Vous pouvez activer l'utilisa tion de jetons dans plusieurs applications protégées en configurant une liste de domaines de jetons pour votre ACL Web.	27 octobre 2022
Toutes les spécifications des en-têtes ne font pas la distincti on majuscules/minuscules	Modification de la spécifica tion de tous les en-têtes pour qu'elle ne distingue pas les majuscules et minuscule s. Cela correspond au comportement de l'en-tête unique.	26 octobre 2022
AWS Firewall Manager modifications de politique gérées	Corrections apportées à`AWSFMAdminFullAcce ss` .	21 octobre 2022

Règles AWS gérées mises à jour pour AWS WAF	Mise à jour du groupe de règles relatives aux entrées erronées connues.	20 octobre 2022
Règles AWS gérées mises à jour pour AWS WAF	Mise à jour du groupe de règles relatives aux entrées erronées connues.	5 octobre 2022
Mise à jour de la AWS WAF spécification du SDK mobile	La valeur par défaut a été abaissée `tokenRefreshDelaySec` de 600 (10 minutes) à 300 (5 minutes).	30 septembre 2022
Règles AWS gérées mises à jour pour AWS WAF	Correction des noms d'étiquettes fournis dans cette documentation pour les groupes de règles suivants : système d'exploitation POSIX, application PHP, WordPress application.	19 septembre 2022
Nouvelle option AWS WAF de règle de politique dans AWS Firewall Manager	AWS Firewall Manager prend désormais en charge les requêtes et réponses Web personnalisées pour les actions Web par défaut dans AWS WAF les politiques.	9 septembre 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : réputation IP.	30 août 2022

AWS WAF modifications de politique gérées	Mis à jour `AWSWAFFullAccessPolicy` `AWSWAFConsoleFullAccess` ,`AWSWAFReadOnlyAccess` , et `AWSWAFConsoleReadOnlyAccess` pour ajouter des groupes d'utilisateurs Amazon Cognito aux types de ressources avec lesquels vous pouvez vous protéger. AWS WAF	25 août 2022
AWS WAF Contrôle des fraudes et prévention des prises de contrôle des comptes (ATP)	Vous pouvez désormais utiliser la fonctionnalité de prévention du rachat de compte AWS WAF Fraud Control (ATP) avec les CloudFront distributions Amazon.	24 août 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : Entrées erronées connues.	22 août 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour :`AWSManagedRulesATPRuleSet` .	11 août 2022

Ajout de la prise en charge des groupes d'utilisateurs Amazon Cognito pour AWS WAF	Vous pouvez désormais associer une ACL AWS WAF Web à un groupe d'utilisateurs Amazon Cognito. Cette modification n'est disponible que dans la dernière version de AWS WAF et non dans AWS WAF Classic.	11 août 2022
Ajout d'une section sur les déploiements pour les groupes de règles AWS gérées versionnés	Ajout d'une nouvelle section documentant les déploiements pour les groupes de règles AWS gérées versionnés. La section inclut des informations sur la façon dont les versions par défaut sont nommées lors des déploiements de versions candidates.	29 juillet 2022
Exigences mises à jour pour configurer la journalisation pour les politiques de Network Firewall	Exigences supplémentaires pour les politiques de Network Firewall qui utilisent un compartiment Amazon S3 chiffré comme destination du journal.	26 juillet 2022
Option de niveau de sensibilité pour l'instruction de règle SQLi	Vous pouvez désormais augmenter la sensibilité de vos instructions de règles d'injection SQL. Cela ne change pas le comportement des instructions existantes, dont le niveau de sensibilité par défaut est deLOW.	15 juillet 2022

Ajout de l'option de configuration de la politique Network Firewall	Firewall Manager prend désormais en charge l'ordre d'évaluation dynamique et les actions par défaut dans les configurations de politique de pare-feu de Network Firewall.	14 juillet 2022
Mises à jour des paramètres des règles de politique de groupe de sécurité de Firewall Manager	Firewall Manager prend désormais en charge la distribution de balises entre les groupes de sécurité principaux et les groupes de sécurité répliqués.	7 juillet 2022
Mises à jour du AWS Shield guide	Les informations contenues dans le guide Shield ont été étendues pour décrire la manière dont Shield atténue les événements.	24 juin 2022
Conseils actualisés pour tester et régler AWS WAF les protections	Les instructions générales pour les tests et les réglages ont AWS WAF été mises à jour et constituent désormais un sujet de premier niveau.	20 juin 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour des groupes de règles suivants : Ensemble de règles de base (CRS).	9 juin 2022
Le nouveau Firewall Manager a confondu les directives de ses adjoints	Ajout de conseils sur la manière d'éviter le problème de confusion lié aux adjoints dans Firewall Manager.	1 juin 2022

Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour des groupes de règles suivants : Ensemble de règles de base (CRS).	24 mai 2022
Nouveaux composants de AWS WAF demande : Headers et Cookies	Vous pouvez désormais inspecter les cookies d'une requête Web et vous pouvez inspecter tous les en-têtes d'une requête Web, en plus d'un seul en-tête.	29 avril 2022
AWS WAF gestion du corps surdimensionné, des en-têtes et des composants de demande de cookies	Vous pouvez désormais spécifier comment AWS WAF gérer les corps de requête, les en-têtes et les cookies surdimensionnés dans le cadre de vos règles qui inspectent ces composant s. Les règles que vous avez déjà créées pour inspecter ces composants ont un comportement qui correspond à la nouvelle Continue option de gestion des surdimens ionnements.	29 avril 2022
AWS WAF Modifications de la politique de journalisation d'Amazon S3	Mise à jour de la politique d'autorisation des journaux Amazon S3 et de son exemple.	12 avril 2022

L'option d'atténuation automatique des attaques DDoS au niveau de la couche applicative est désormais disponible avec AWS Shield Advanced Application Load Balancer	Shield Advanced prend désormais en charge l'atténuation automatique des attaques DDoS au niveau de la couche application pour les équilibreurs de charge des applications, ce qui le rend disponible pour toutes les protections de la couche application. Vous pouvez configurer Shield Advanced pour compter ou bloquer automatiquement les requêtes Web qui font partie d'une attaque DDoS de la couche application contre une ressource protégée.	8 avril 2022
Ajout d'un indicateur du paramètre de version par défaut actuel pour les groupes de règles gérés	Les listes de versions des groupes de règles gérés indiquent désormais quelle version est actuellement la version par défaut.	8 avril 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : AWS WAF Bot Control.	6 avril 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : Entrées erronées connues.	31 mars 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : Entrées erronées connues.	30 mars 2022

Firewall Manager ajoute la prise en charge du pare-feu de nouvelle génération (NGFW) dans le cloud de Palo Alto Networks	Firewall Manager prend désormais en charge le pare-feu de nouvelle génération (NGFW) dans le cloud de Palo Alto Networks.	30 mars 2022
Ajoutez le support pour Palo Alto Networks Cloud NGFW à AWS Firewall Manager	AWS Firewall Manager prend désormais en charge les politiques de pare-feu de nouvelle génération (NGFW) de Palo Alto Networks Cloud.	30 mars 2022
Mises à jour du AWS Shield guide	Les informations contenues dans le guide Shield ont été étendues pour décrire la manière dont Shield détecte les événements et pour fournir des exemples d'architectures résilientes aux attaques DDoS.	16 mars 2022
Mises à jour du AWS Shield guide	Élargissement des informations contenues dans le guide Shield et amélioration de l'organisation des différentes sections. Les principales modifications concernent les sections suivantes du guide Shield : support de la Shield Response Team (SRT), protection des ressources lors des événements DDoS et visibilité sur les événements DDoS. AWS Shield Advanced	28 février 2022

Firewall Manager prend désormais en charge le modèle de déploiement centralisé de Network Firewall	Ajout d'une nouvelle procédure qui explique comment configurer des politiques utilisant des modèles de déploiement distribués et centralisés.	24 février 2022
Firewall Manager ajoute la prise en charge du modèle de déploiement AWS Network Firewall centralisé	Vous pouvez désormais configurer vos AWS Network Firewall politiques pour utiliser le modèle de déploiement distribué ou centralisé. Avec le modèle de déploiement distribué, Firewall Manager crée et gère des points de terminaison de pare-feu dans chaque VPC relevant du champ d'application de la politique. Avec le modèle de déploiement centralisé, Firewall Manager crée et gère les points de terminaison du pare-feu dans un seul VPC d'inspection.	24 février 2022
Ajoutez la prise en charge du versionnement des groupes de règles AWS WAF gérés à AWS Firewall Manager	AWS Firewall Manager prend désormais en charge le versionnement des groupes de règles AWS WAF gérés dans les AWS WAF politiques de Firewall Manager.	18 février 2022
AWS Firewall Manager changement de politique géré	Mettre à jour vers`FMSServiceRolePolicy` .	16 février 2022

Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : listes de réputation IP.	15 février 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour AWS WAF ajouter le groupe de règles de prévention du piratage de comptes AWS WAF Fraud Control (ATP)`AWSManagedRulesATPRuleSet` .	11 février 2022
Modifications apportées à l'organisation du AWS WAF guide	Ajout d'une nouvelle section de haut niveau pour les protections gérées. La section CAPTCHA a été déplacée de la section « règles » vers la nouvelle section « protections gérées ». La section des étiquettes a été déplacée de la section « under rules » vers sa propre section de niveau supérieur.	11 février 2022
AWS WAF intégrations d'applications clientes	Utilisez les API client AWS WAF JavaScript et mobile pour intégrer vos applications clientes aux groupes de règles AWS Managed Rules d'atténuation intelligente des menaces afin d'améliorer la détection.	11 février 2022

AWS WAF Contrôle des fraudes et prévention des prises de contrôle des comptes (ATP)	Vous pouvez détecter et bloquer les tentatives de prise de contrôle de compte grâce au nouveau groupe de règles géré AWS WAF Fraud Control Account Takeover Prevention (ATP)`AWSManagedRulesATPRuleSet` .	11 février 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : Entrées erronées connues.	28 janvier 2022
AWS WAF modifications de politique gérées	Mis à jour `AWSWAFFullAccessPolicy` et `AWSWAFConsoleFullAccess` pour corriger les autorisations de journalisation.	11 janvier 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : ensemble de règles de base (CRS), base de données SQLi.	10 janvier 2022
Firewall Manager prend en charge l'atténuation automatique des attaques DDoS au niveau de la couche applicative Shield Advanced	Les politiques avancées de Firewall Manager Shield pour les CloudFront ressources Amazon incluent désormais la prise en charge de l'atténuation automatique des attaques DDoS au niveau de la couche application.	7 janvier 2022

AWS Firewall Manager changement de politique géré	Mettre à jour vers`FMSServiceRolePolicy` .	7 janvier 2022
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : Entrées erronées connues.	17 décembre 2021
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : Entrées erronées connues.	11 décembre 2021
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : Entrées erronées connues.	10 décembre 2021
Nouveau rôle AWS Shield Advanced lié au service	Ajouté `AWSServiceRoleForAWSShield` pour prendre en charge la fonctionnalité d'atténuation automatique des attaques DDoS au niveau de la couche d'application.	1er décembre 2021
Nouvelle politique AWS Shield gérée	Ajouté `AWSShieldServiceRolePolicy` pour prendre en charge la fonctionnalité d'atténuation automatique des attaques DDoS au niveau de la couche d'application.	1er décembre 2021

L'option d'atténuation automatique des attaques DDoS au niveau de la couche applicative est désormais disponible avec for AWS Shield Advanced CloudFront	Shield Advanced prend désormais en charge l'atténuation automatique des attaques DDoS au niveau de la couche application pour les CloudFront distributions Amazon. Vous pouvez configurer Shield Advanced pour compter ou bloquer automatiquement les requêtes Web qui font partie d'une attaque DDoS au niveau de la couche application contre une CloudFront distribution.	1er décembre 2021
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour les groupes de règles suivants AWS WAF mis à jour : ensemble de règles de base (CRS), système d'exploitation Windows, système d'exploitation Linux et listes de réputation IP.	23 novembre 2021
AWS Firewall Manager changement de politique géré	Mettre à jour vers`FMSServiceRolePolicy` .	18 novembre 2021

Options de journalisation étendues pour AWS WAF	Vous pouvez désormais enregistrer le trafic ACL Web dans un groupe de CloudWatch journaux Amazon Logs ou dans un compartiment Amazon Simple Storage Service (Amazon S3). Ces options s'ajoutent à l'option existante de connexion à un flux de diffusion Amazon Data Firehose.	15 novembre 2021
AWS WAF modifications de politique gérées	Mis à jour `AWSWAFFullAccessPolicy` et `AWSWAFConsoleFullAccess` pour prendre en charge des destinations de journalisation supplémentaires.	15 novembre 2021
AWS WAF nouvelle option d'action de CAPTCHA règle	Vous pouvez configurer des règles pour exécuter un CAPTCHA sur des requêtes Web et, le cas échéant, envoyer un problème de CAPTCHA au client.	8 novembre 2021
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles de base (CRS).	27 octobre 2021

Règles AWS gérées mises à jour pour AWS WAF	Tous les groupes de règles AWS gérées prennent désormais en charge l'étiquetage. Les descriptions des règles incluent les spécifications des étiquettes.	25 octobre 2021
Firewall Manager prend en charge le filtrage des journaux de Network Firewall	AWS Firewall Manager prend désormais en charge le filtrage des journaux pour les politiques de Network Firewall.	4 octobre 2021
AWS Firewall Manager changement de politique géré	Mettre à jour vers`FMSServiceRolePolicy` .	29 septembre 2021
Ajout d'une déclaration de match regex	Vous pouvez désormais associer les requêtes Web à une seule expression régulière .	22 septembre 2021
Règles basées sur le taux au sein des groupes AWS WAF de règles	Vous pouvez désormais définir des règles basées sur le taux au sein AWS WAF de groupes de règles. En AWS Firewall Manager, cette fonctionnalité est entièrement prise en charge pour AWS WAF les politiques.	13 septembre 2021
Firewall Manager prend en charge AWS WAF le filtrage des journaux	AWS Firewall Manager prend désormais en charge le filtrage des journaux pour AWS WAF les politiques.	31 août 2021

Supprimer automatiquement les protections out-of-scope des ressources dans AWS Firewall Manager	AWS Firewall Manager vous permet de supprimer automatiquement les protections des ressources qui n'entrent pas dans le champ d'application de la politique.	25 août 2021
AWS Firewall Manager changement de politique géré	Mettre à jour vers`FMSServiceRolePolicy` .	12 août 2021
Ajout du versionnement aux groupes de règles gérés	Les fournisseurs de groupes de règles gérés peuvent désormais versionner leurs groupes de règles.	9 août 2021
Modifier les exigences de AWS Firewall Manager l'administrateur	Vous pouvez utiliser le compte de gestion de l'organisation en tant que compte administrateur de Firewall Manager. Cela avait été interdit.	2 août 2021
Augmentation du quota de Firewall Manager	Le nombre d'instances Amazon VPC que vous pouvez avoir dans le cadre d'une politique Firewall Manager a été augmenté de 10 à 100.	28 juillet 2021

AWS Firewall Manager prise en charge de la surveillance des tables de AWS Network Firewall routage	AWS Firewall Manager prend désormais en charge la surveillance des tables de routage et fournit des recommandations de mesures correctives aux administr ateurs de sécurité pour les AWS Network Firewall politiques impliquant des itinéraires mal configurés.	8 juillet 2021
AWS WAF options de transformation de texte supplémentaires	Options étendues pour les transformations de texte, que vous pouvez appliquer aux composants de requête Web avant de les inspecter.	24 juin 2021
Modification du nom des ressources de AWS WAF politique de Firewall Manager	Le nom des ACL Web, des groupes de règles et de la journalisation gérés par Firewall Manager pour vos AWS WAF politiques a changé.	26 mai 2021
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour une prise en charge AWS WAF accrue de l'étiquetage dans les listes de réputation IP et suppression des suffixes sur les noms de règles pour les listes de réputation IP Amazon.	4 mai 2021

Ajout de la prise en charge de l'administrateur AWS Organizations délégué	Lorsque vous définissez le compte AWS Firewall Manager administrateur, Firewall Manager désigne désormais le compte en tant qu'administrateur AWS Organizations délégué de Firewall Manager. Avec cette modification, lorsque vous définissez le compte administrateur de Firewall Manager, vous devez fournir un compte de membre autre que le compte de gestion de l'organisation. Cette modification n'affecte pas vos paramètres existants.	30 avril 2021
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour AWS WAF ajouter le groupe de règles AWS WAF Bot Control.	1 avril 2021
Définissez des actions de règle individuelles Count dans un groupe de règles	Vous pouvez désormais définir les actions de règle individuelles d'un groupe de règles surCount. Les informations relatives à la dérogation existante, qui se situe au niveau du groupe de règles, ont été corrigées.	1 avril 2021

Déclaration de portée réduite pour les groupes de règles gérés	Vous pouvez désormais utiliser une instruction de portée réduite avec des groupes de règles gérés de la même manière qu'avec une instruction basée sur des taux.	1 avril 2021
Filtrage des journaux	Vous pouvez désormais filtrer le trafic ACL Web que vous enregistrez en fonction de l'action des règles et de l'étiquette.	1 avril 2021
AWS WAF étiquettes sur les requêtes Web	Vous pouvez configurer des règles pour ajouter des étiquettes aux requêtes Web correspondantes et pour faire correspondre les étiquettes ajoutées par d'autres règles.	1 avril 2021
AWS WAF Contrôle des robots	Vous pouvez surveiller et contrôler le trafic des bots grâce à la nouvelle fonctionn alité AWS WAF Bot Control, qui combine le groupe de règles géré par Bot Control avec l'étiquetage des requêtes Web, les instructions de délimitation et le filtrage des journaux.	1 avril 2021
Firewall Manager prend en charge les politiques de pare-feu DNS d'Amazon Route 53 Resolver	AWS Firewall Manager prend en charge la gestion centralis ée du filtrage du trafic DNS sortant du pare-feu DNS Amazon Route 53 Resolver pour vos VPC.	31 mars 2021

Gestion personnalisée des demandes et des réponses	Vous pouvez inclure des en-têtes personnalisés pour les requêtes Web qui AWS WAF ne bloquent pas et vous pouvez envoyer des réponses personnalisées pour les demandes Web qui AWS WAF bloquent. Ceci est disponible pour les paramètres d'action par défaut et d'action de règle de l'ACL Web.	29 mars 2021
AWS Firewall Manager changement de politique géré	Mettre à jour vers`FMSServiceRolePolicy` .	17 mars 2021
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour des groupes de règles suivants : ensemble de règles de base (CRS), protection de l'administrateur, entrées erronées connues et système d'exploitation Linux.	3 mars 2021
AWS Shield suivi géré des modifications des politiques	Shield a commencé à suivre les modifications apportées AWS à ses politiques gérées.	3 mars 2021
AWS Firewall Manager suivi géré des modifications des politiques	Firewall Manager a commencé à suivre les modifications apportées AWS à ses politiques gérées.	2 mars 2021
AWS WAF suivi géré des modifications des politiques	AWS WAF a commencé à suivre les modifications apportées AWS à ses politiques gérées.	1er mars 2021

Inspecter le corps d'une requête Web en tant que JSON analysé	Ajout de l'option permettant d'inspecter le corps de la requête Web sous forme de JSON analysé et filtré. Cela s'ajoute à l'option existante permettant d'inspecter le corps de la requête Web sous forme de texte brut.	12 février 2021
Firewall Manager prend en charge AWS Network Firewall les politiques	AWS Firewall Manager prend en charge la gestion centralisée du filtrage du trafic AWS Network Firewall réseau pour vos VPC.	17 novembre 2020
Ajouter la prise en charge des groupes AWS Shield Advanced de protection	Vous pouvez désormais regrouper vos ressources protégées en groupes logiques et gérer leurs protections collectivement.	13 novembre 2020
Ajout de la prise en charge AWS AppSync de AWS WAF	Vous pouvez désormais associer une ACL AWS WAF Web à votre API AWS AppSync GraphQL. Cette modification n'est disponible que dans la dernière version de AWS WAF et non dans AWS WAF Classic.	1er octobre 2020
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour mettre AWS WAF à jour l'ensemble de règles du système d'exploitation Windows.	23 septembre 2020

Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour des ensembles de règles, de l'application PHP et du système d'exploitation POSIX.	16 septembre 2020
AWS Shield Console mise à jour	AWS Shield propose une nouvelle option de console, avec une expérience utilisateur améliorée. Les instructions relatives à la console figurant dans la documentation concernent la nouvelle console.	1 septembre 2020
Firewall Manager met à jour les politiques communes des groupes de sécurité	AWS Firewall Manager les politiques communes des groupes de sécurité prennent désormais en charge les types de ressources des équilibreurs de charge d'application et des équilibreurs de charge classiques via la mise en œuvre de la console. Les nouvelles options sont disponibles dans les paramètres de portée de la politique commune.	11 août 2020
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour mettre AWS WAF à jour l'ensemble de règles de base.	7 août 2020

Firewall Manager prend en charge la configuration de la AWS WAF journalisation	AWS Firewall Manager prend désormais en charge la configuration de journalisation centralisée pour AWS WAF les politiques.	30 juillet 2020
Spécifier l'emplacement de l'adresse IP dans la requête Web	Ajout de l'option permettant d'utiliser les adresses IP d'un en-tête HTTP que vous spécifiez, au lieu d'utiliser l'origine de la requête Web. L'en-tête secondaire est généralement `X-Forwarded-For` (XFF), mais vous pouvez spécifier n'importe quel nom d'en-tête. Vous pouvez utiliser cette option pour la mise en correspondance d'ensembles d'adresses IP, la correspondance géographique et l'agrégation du nombre de règles basée sur le taux.	9 juillet 2020
Firewall Manager met à jour les politiques des groupes de sécurité en matière d'audit de contenu	AWS Firewall Manager propose des fonctionnalités étendues pour les politiques de groupe de sécurité relatives à l'audit de contenu, notamment une option de règles gérées, qui utilise des listes d'applications et de protocoles gérés, ainsi que des informations sur les violations de ressources.	7 juillet 2020

Listes gérées par Firewall Manager	AWS Firewall Manager prend désormais en charge les listes d'applications et de protocoles gérés. Firewall Manager gère certaines listes et vous pouvez créer et gérer les vôtres.	7 juillet 2020
Firewall Manager prend en charge les VPC partagés dans le cadre de politiques de groupe de sécurité communes	AWS Firewall Manager prend désormais en charge l'utilisation de politiques de groupe de sécurité communes dans les VPC partagés. Vous pouvez le faire en plus de les utiliser dans les VPC appartenant à des comptes concernés.	26 mai 2020
Règles AWS gérées mises à jour pour AWS WAF	Ajout de documentation pour chaque règle dans les règles AWS gérées pour AWS WAF.	20 mai 2020
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour la AWS WAF mise à jour du groupe de règles du système d'exploitation Linux.	19 mai 2020
Ajout de la prise en charge de la migration des ressources AWS WAF classiques vers AWS WAF (v2)	Vous pouvez désormais utiliser la console ou l'API pour exporter vos ressources AWS WAF Classic afin de les migrer vers la dernière version de AWS WAF.	27 avril 2020

Ajouter la prise en charge des unités AWS Organizations organisationnelles dans le champ d'application de la politique	AWS Firewall Manager prend désormais en charge l'utilisation AWS Organizations d'unités organisationnelles (UO) pour spécifier le champ d'application de la politique. Vous pouvez utiliser des unités d'organisation pour inclure ou exclure des comptes de la portée, en plus d'inclure ou d'exclure des comptes spécifiques. Spécifier une unité d'organisation équivaut à spécifier tous les comptes de l'unité d'organisation et, le cas échéant, les unités d'organisation enfants, y compris les unités d'organisation enfants et les comptes ajoutés ultérieurement.	6 avril 2020
Ajouter le support pour AWS WAF (v2) à AWS Firewall Manager	AWS Firewall Manager prend désormais en charge la dernière version de AWS WAF Classic AWS WAF, en plus de la version précédente.	31 mars 2020

Mise à jour des politiques AWS Firewall Manager communes des groupes de sécurité	AWS Firewall Manager Common Security Group Policy a désormais la possibilité d'appliquer cette politique à toutes les interfaces réseau élastiques de vos instances Amazon EC2 incluses. Vous pouvez toujours choisir d'appliquer la stratégie uniquement à l'interface réseau Elastic par défaut.	11 mars 2020
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour AWS WAF ajouter un groupe de `AWSManagedRulesAnonymousIpList` règles.	6 mars 2020
Règles AWS gérées mises à jour pour AWS WAF	AWS Règles gérées pour mettre AWS WAF à jour l'WordPress application et les groupes de `AWSManagedRulesCommonRuleSet` règles.	3 mars 2020
Ajout de la vérification de l'état d'Amazon Route 53 aux options AWS Shield Advanced de protection	Shield Advanced prend désormais en charge l'utilisation des associations de contrôle de santé d'Amazon Route 53, afin d'améliorer la précision de la détection et de l'atténuation des menaces.	14 février 2020
Règles AWS gérées mises à jour pour AWS WAF	AWS Managed Rules for AWS WAF a mis à jour le groupe de règles de la base de données SQL pour ajouter la vérification de l'URI du message.	23 janvier 2020

Firewall Manager : nouvelle option pour la politique d'audit de l'utilisation des groupes de sécurité	Firewall Manager propose une nouvelle option pour les politiques d'audit de l'utilisation des groupes de sécurité. Vous pouvez maintenant définir un nombre minimum de minutes d'inutilisation d'un groupe de sécurité au-delà duquel il sera considéré comme non conforme. Par défaut, ce paramètre est égal à 0 minute.	14 janvier 2020
Firewall Manager : nouvelle option pour les AWS WAF politiques	Firewall Manager propose une nouvelle option pour les AWS WAF politiques. Vous pouvez désormais choisir de supprimer toutes les associations ACL web existantes des ressources concernées avant d'y associer les nouvelles ACL web de la stratégie.	14 janvier 2020
Règles AWS gérées mises à jour pour AWS WAF	AWS Managed Rules for AWS WAF a mis à jour les transformations de texte pour les règles du jeu de règles de base et des groupes de règles de base de données SQL.	20 décembre 2019
AWS Firewall Manager intégré à AWS Security Hub	AWS Firewall Manager crée désormais des résultats pour les ressources non conformes et pour les attaques et les envoie à AWS Security Hub.	18 décembre 2019

Sortie de la AWS WAF version 2	Nouvelle version du guide du AWS WAF développeur. Vous pouvez gérer une liste ACL web ou un groupe de règles au format JSON. Les fonctionnalités étendues incluent les instructions de règle logique, l'imbrication d'instructions de règle et la prise en charge CIDR complète des adresses IP et des plages d'adresses. Les règles ne sont plus AWS des ressources, elles n'existent que dans le contexte d'une ACL Web ou d'un groupe de règles. Pour les clients existants, la version précédente du service s'appelle désormais AWS WAF Classic. Dans les API, les SDK et les CLI, AWS WAF Classic conserve ses schémas de dénomination et cette dernière version de AWS WAF est désignée par un « V2 » ou « v2 » ajouté, selon le contexte. AWS WAF ne peut pas accéder aux AWS ressources créées dans AWS WAF Classic. Pour utiliser ces ressources dans AWS WAF, vous devez les migrer.	25 novembre 2019
AWS Groupes de règles gérées pour AWS WAF	Ajout de groupes de règles AWS gérées. Ils sont gratuits pour les AWS WAF clients.	25 novembre 2019

AWS Firewall Manager prise en charge des groupes de sécurité Amazon Virtual Private Cloud	La prise en charge des groupes de sécurité Amazon VPC a été ajoutée à Firewall Manager.	10 octobre 2019
AWS Firewall Manager support pour AWS Shield Advanced	Ajout de la prise en charge de Shield Advanced à Firewall Manager.	15 mars 2019
Tutoriel : Création de politiques hiérarchiques	Ajout d'un didacticiel sur la création de stratégies hiérarchiques dans AWS Firewall Manager.	11 février 2019
Contrôle au niveau des règles dans les groupes de règles	Vous pouvez désormais exclure des règles individuelles des groupes de AWS Marketplace règles, ainsi que vos propres groupes de règles.	12 décembre 2018
AWS Shield Advanced support pour les accélérateurs AWS Global Accelerator standard	Shield Advanced peut désormais protéger les accélérateurs AWS Global Accelerator standard.	26 novembre 2018
AWS WAF prise en charge d'Amazon API Gateway	AWS WAF protège désormais les API Amazon API Gateway.	le 25 octobre 2018
Assistant de démarrage avancé avec Expanded AWS Shield	Le nouvel assistant permet de créer des règles basées sur les taux et Amazon CloudWatch Events.	31 août 2018

AWS WAF logging	Activez la journalisation pour obtenir des informations détaillées sur le trafic qui est analysé par votre liste ACL web.	31 août 2018
Support des paramètres de requête dans les conditions	Lorsque vous créez une condition, vous pouvez désormais effectuer une recherche parmi les requêtes pour trouver des paramètres spécifiques.	5 juin 2018
Assistant de démarrage avancé de Shield	Introduit un nouveau processus simplifié pour s'abonner à AWS Shield Advanced.	5 juin 2018
Plages CIDR autorisées étendues	Lors de la création d'une condition de correspondance IP, elle prend AWS WAF désormais en charge les plages d'adresses IPv4 : /8 et toute plage comprise entre /16 et /32.	5 juin 2018

Mises à jour avant 2018

Le tableau suivant décrit les modifications importantes apportées à chaque version du Guide du AWS WAF développeur avant 2018.

Modification	Version de l'API	Description	Date de parution
Mettre à jour	2016-08-24	AWS Marketplace groupes de règles	Novembre 2017

Modification	Version de l'API	Description	Date de parution
Mettre à jour	2016-08-24	Support avancé Shield pour les adresse IP Elastic	Novembre 2017
Mettre à jour	2016-08-24	Tableau de bord des menaces mondiales	Novembre 2017
Mettre à jour	2016-08-24	Didacticiel de site web résistant aux attaques DDoS	Octobre 2017
Mettre à jour	2016-08-24	Conditions d'emplacement géographique et d'expressions régulières	Octobre 2017
Mettre à jour	2016-08-24	Règles basées sur un débit	Juin 2017
Mettre à jour	2016-08-24	Réorganisation	Avril 2017
Mettre à jour	2016-08-24	Ajout d'informations sur la protection DDOS et la prise en charge d'équilibreurs de charge d'application.	Novembre 2016

Modification	Version de l'API	Description	Date de parution
Nouvelles fonctions	24-08-2015	Vous pouvez désormais enregistrer tous vos appels d'API à AWS WAF through AWS CloudTrail, le AWS service qui enregistre les appels d'API pour votre compte et envoie les fichiers journaux à votre compartiment S3. CloudTrail les journaux peuvent être utilisés pour effectuer des analyses de sécurité, suivre les modifications apportées à vos AWS ressources et faciliter l'audit de conformité. L'intégration AWS WAF vous CloudTrail permet de déterminer quelles demandes ont été adressées à l' AWS WAF API, l'adresse IP source à partir de laquelle chaque demande a été faite, qui a fait la demande, quand elle a été faite, etc. Si vous l'utilisez déjà AWS CloudTrail, vous commencerez à voir des appels AWS WAF d'API dans votre CloudTrail journal. Si vous n'avez pas activé CloudTrail votre compte, vous pouvez l'activer CloudTrail depuis le AWS Management Console. L'activation n'entraîne aucun frais supplémentaire CloudTrail, mais les tarifs standard pour l'utilisation d'Amazon S3 et d'Amazon SNS s'appliquent.	28 avril 2016
Nouvelles fonctions	24-08-2015	Vous pouvez désormais l'utiliser AWS WAF pour autoriser, bloquer ou compter les requêtes Web qui semblent contenir des scripts malveillants, ce que l'on appelle le cross-site scripting ou XSS. Les pirates insèrent parfois des scripts malveillants dans les requêtes web dans le but d'exploiter les vulnérabilités d'applications web. Pour plus d'informations, consultez Instruction d'attaque par scripts inter-site de règle.	29 mars 2016

Modification	Version de l'API	Description	Date de parution
Nouvelles fonctions	24-08-2015	Avec cette version, les AWS WAF fonctionnalités suivantes sont ajoutées : • Vous pouvez configurer AWS WAF pour autoriser , bloquer ou compter les requêtes Web en fonction de la longueur des parties spécifiées des demandes, telles que les chaînes de requête ou les URI. Pour plus d'informations, consultez Instruction de contrainte de taille de règle. • Vous pouvez configurer AWS WAF pour autoriser , bloquer ou compter les requêtes Web en fonction du contenu du corps de la demande. C'est la partie d'une requête qui contient les données supplémentaires que vous souhaitez envoyer à votre serveur web en tant que corps de la requête HTTP, telles que les données d'un formulaire. Cette fonctionnalité s'applique aux conditions de correspondance de chaîne, aux conditions de correspondance d'injection SQL et aux nouvelles conditions de contrainte de taille mentionnées au premier point. Pour plus d'informations, consultez Spécification et gestion des composants de requête Web.	27 janvier 2016
Nouvelle fonction	24-08-2015	Vous pouvez désormais utiliser la AWS WAF console pour choisir les CloudFront distributions auxquelles vous souhaitez associer une ACL Web. Pour plus d'informations, consultez la section Association ou dissociation d'une ACL Web et d'une CloudFront distribution.	16 novembre 2015
Première version	24-08-2015	Il s'agit de la première version du Guide du développeur AWS WAF .	6 octobre 2015

AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le AWS glossaire dans la Glossaire AWS référence.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.