Guide de mise en œuvre

Automatisations de sécurité pour AWS WAF

Automatisations de sécurité pour AWS WAF: Guide de mise en œuvre

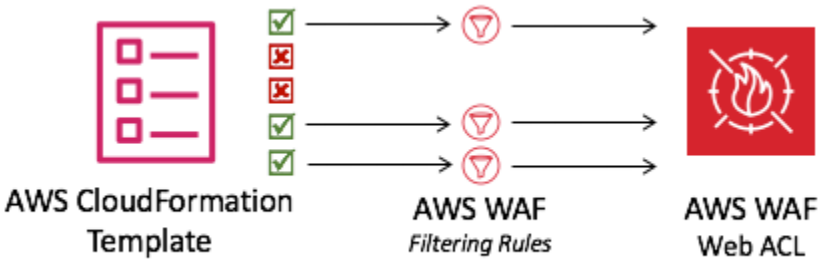
Table of Contents

Déployez automatiquement une liste de contrôle d'accès Web unique qui filtre les attaques Web grâce aux automatisations de sécurité sur AWS WAF

La solution Security Automations for AWS WAF déploie un ensemble de règles préconfigurées pour vous aider à protéger vos applications contre les exploits Web courants. Le service principal de cette solution, AWS WAF, aide à protéger les applications Web contre les techniques d'attaque susceptibles d'affecter la disponibilité des applications, de compromettre la sécurité ou de consommer des ressources excessives. Vous pouvez utiliser AWS WAF pour définir des règles de sécurité Web personnalisables. Ces règles contrôlent le trafic à autoriser ou à bloquer vers les applications Web et les interfaces de programmation d'applications (APIs) déployées sur des ressources AWS telles qu'Amazon CloudFront, Application Load Balancer (ALB). Pour d'autres types de ressources pris en charge, consultez AWS WAF dans le manuel AWS WAF, AWS Firewall Manager et AWS Shield Advanced Developer Guide.

La configuration des règles AWS WAF peut s'avérer difficile et fastidieuse pour les grandes comme pour les petites entreprises, en particulier pour celles qui ne disposent pas d'équipes de sécurité dédiées. Pour simplifier ce processus, la solution Security Automations for AWS WAF déploie automatiquement une liste de contrôle d'accès Web (ACL) unique avec un ensemble de règles AWS WAF conçues pour filtrer les attaques Web courantes. Lors de la configuration initiale du CloudFormation modèle AWS de cette solution, vous pouvez spécifier les fonctionnalités de protection à inclure. Une fois que vous avez déployé cette solution, AWS WAF inspecte les requêtes Web adressées à leurs CloudFront distributions ou ALB existants, et les bloque le cas échéant.

Un CloudFormation modèle déploie une ACL Web avec des règles de filtrage AWS WAF.



Ce guide de mise en œuvre aborde les considérations architecturales, les étapes de configuration et les meilleures pratiques opérationnelles pour déployer cette solution dans le cloud Amazon Web

Services (AWS). Il inclut des liens vers des CloudFormation modèles qui lancent, configurent et exécutent les services de sécurité, de calcul, de stockage et autres services AWS nécessaires au déploiement de cette solution sur AWS, en utilisant les meilleures pratiques d'AWS en matière de sécurité et de disponibilité.

Les informations contenues dans ce guide supposent une connaissance pratique des services AWS tels qu'AWS WAF, CloudFront ALBs, et AWS Lambda. Cela nécessite également des connaissances de base sur les attaques Web courantes et les stratégies d'atténuation.

> **Note**
>
> Depuis la version 3.0.0, cette solution prend en charge la dernière version de l'API de service AWS WAF (AWS WAFV2).

Ce guide est destiné aux responsables informatiques, aux ingénieurs en sécurité, aux DevOps ingénieurs, aux développeurs, aux architectes de solutions et aux administrateurs de sites Web.

> **Note**
>
> Nous vous recommandons d'utiliser cette solution comme point de départ pour la mise en œuvre des règles AWS WAF. Vous pouvez personnaliser le code source, ajouter de nouvelles règles personnalisées et tirer parti d'un plus grand nombre de règles gérées par AWS WAF en fonction de vos besoins.

Utilisez ce tableau de navigation pour trouver rapidement les réponses aux questions suivantes :

Si tu veux...	Lisez.
Connaissez le coût de fonctionnement de cette solution. Le coût total de fonctionnement de cette solution dépend de la protection activée et de la quantité de données ingérées, stockées et traitées.	Coût
Comprenez les considérations de sécurité liées à cette solution.	Sécurité

Si tu veux...	Lisez.
Découvrez quelles régions AWS sont prises en charge pour cette solution.	Régions AWS prises en charge
Consultez ou téléchargez le CloudFormation modèle inclus dans cette solution pour déployer automatiquement les ressources d'infrast ructure (la « pile ») de cette solution.	CloudFormation Modèle AWS
Utilisez le Support pour vous aider à déployer, utiliser ou dépanner la solution.	Support
Accédez au code source et utilisez éventuell ement l'AWS Cloud Development Kit (AWS CDK) pour déployer la solution	GitHub référentiel

Fonctionnalités et avantages

La solution Security Automations for AWS WAF fournit les fonctionnalités et avantages suivants.

Sécurisez vos applications Web avec les groupes de règles AWS Managed Rules

Les règles gérées par AWS pour AWS WAF fournissent une protection contre les vulnérabilités courantes des applications ou contre tout autre trafic indésirable. Cette solution inclut les groupes de règles de réputation IP gérés par AWS, les groupes de règles de base AWS Managed et les groupes de règles spécifiques aux cas d'utilisation AWS Managed. Vous avez la possibilité de sélectionner un ou plusieurs groupes de règles pour votre ACL Web, dans la limite du quota d'unités de capacité maximale de l'ACL Web (WCU).

Fournir une protection contre les inondations de couche 7 avec une règle personnalisée HTTP Flood prédéfinie

La règle personnalisée HTTP Flood protège contre une attaque distribuée Denial-of-Service (DDoS) sur la couche Web pendant une période définie par le client. Vous pouvez choisir l'une des options suivantes pour activer cette règle :

- Règle basée sur le taux AWS WAF
- Analyseur de log Lambda
- Analyseur de journaux Amazon Athena

Les options Lambda log parser ou Athena log parser vous permettent de définir un quota de requêtes inférieur à 100. Cette approche peut vous aider à ne pas atteindre le quota requis par les règles basées sur le taux d'AWS WAF. Pour plus d'informations, consultez la section Options de l'analyseur de log.

Vous pouvez également améliorer l'analyseur de log Athena en ajoutant un pays et un identifiant de ressource uniforme (URI) aux conditions de filtrage. Cette approche identifie et bloque les attaques HTTP Flood dont les modèles d'URI sont imprévisibles. Pour plus d'informations, reportez-vous à la section Utiliser le pays et l'URI dans l'analyseur de journaux HTTP Flood Athena.

Bloquez l'exploitation des vulnérabilités grâce à une règle personnalisée prédéfinie pour Scanners & Probes

La règle personnalisée Scanners & Probes analyse les journaux d'accès aux applications à la recherche de comportements suspects, tels qu'un nombre anormal d'erreurs générées par une origine. Il bloque ensuite ces adresses IP sources suspectes pendant une période définie par le client. Vous pouvez choisir l'une des options suivantes pour activer cette règle : Lambda log parser ou Athena log parser. Pour plus d'informations, consultez la section Options de l'analyseur de log.

Détectez et bloquez les intrusions grâce à la règle personnalisée Bad Bot prédéfinie

La règle personnalisée Bad Bot définit un point de terminaison honeypot, qui est un mécanisme de sécurité destiné à attirer et à déjouer une tentative d'attaque. Vous pouvez insérer le point de terminaison dans votre site Web pour détecter les demandes entrantes provenant des scrapeurs de contenu et des robots malveillants. Une fois détectée, toutes les demandes ultérieures provenant des mêmes origines seront bloquées. Pour plus d'informations, voir Intégrer le lien Honeypot dans votre application Web.

Bloquer les adresses IP malveillantes avec des règles personnalisées de listes de réputations IP prédéfinies

La règle personnalisée des listes de réputation IP vérifie toutes les heures les listes de réputation IP tierces pour détecter les nouvelles plages d'adresses IP à bloquer. Ces listes incluent les listes Do't Route Or Peer (DROP) et Extended DROP (EDROP) de Spamhaus, la liste IP des menaces émergentes de Proofpoint et la liste des nœuds de sortie Tor.

Fournir une configuration IP manuelle avec une règle personnalisée prédéfinie pour les listes d'adresses IP autorisées et refusées

Les règles personnalisées des listes d'adresses IP autorisées et refusées vous permettent d'insérer manuellement les adresses IP que vous souhaitez autoriser ou refuser. Vous pouvez également configurer la rétention des adresses IP sur les listes d'adresses IP autorisées et refusées pour qu'elles expirent IPs à une heure définie.

Créez votre propre tableau de bord de surveillance

Cette solution émet des CloudWatch métriques Amazon telles que les demandes autorisées, les demandes bloquées et d'autres métriques pertinentes. Vous pouvez créer un tableau de bord personnalisé pour visualiser ces indicateurs et obtenir des informations sur le schéma des attaques et la protection fournie par AWS WAF. Pour plus d'informations, reportez-vous à la section Créer un tableau de bord de surveillance.

Cas d’utilisation

Voici des exemples de cas d'utilisation de cette solution. Vous pouvez personnaliser cette solution de manière innovante qui ne se limite pas à cette liste.

Automatisez la configuration des règles AWS WAF

AWS WAF protège votre application Web contre les attaques courantes ; toutefois, la configuration des règles AWS WAF peut s'avérer complexe et chronophage. Pour vous aider, cette solution déploie automatiquement un ensemble de règles AWS WAF dans votre compte à l'aide CloudFormation d'un modèle. Ainsi, vous n'avez pas besoin de configurer vous-même les règles d'AWS WAF et vous pouvez commencer à utiliser AWS WAF plus rapidement.

Personnalisez la protection HTTP Flood de couche 7

Cette solution propose trois options pour activer la protection HTTP Flood. Vous pouvez sélectionner l'option qui correspond à vos besoins pour vous protéger contre les attaques DDo S. Pour plus d'informations, voir Fournir une protection contre les inondations de couche 7 avec une règle personnalisée HTTP Flood prédéfinie dans Fonctionnalités et avantages.

Tirez parti du code source pour appliquer la personnalisation ou créer vos propres automatisations de sécurité

Cette solution fournit un exemple d'utilisation d'AWS WAF et d'autres services pour créer des automatisations de sécurité sur le cloud AWS. Son code source ouvert vous GitHub permet d'appliquer facilement des personnalisations ou de créer vos propres automatisations de sécurité adaptées à vos besoins.

Concepts et définitions

Cette section décrit les concepts clés et définit la terminologie spécifique à cette solution.

Journaux ALB

Cette solution utilise des journaux pour la ressource ALB. La règle de protection des scanners et des sondes de cette solution inspecte ces journaux.

Analyseur de log Athena

Amazon Athena est un service d'analyse interactif sans serveur qui repose sur des frameworks open source et prend en charge les formats de fichier et de table ouverts. Cette solution exécute une requête Athena planifiée pour inspecter les journaux AWS CloudFront, WAF ou ALB si l'utilisateur le `yes - Amazon Athena log parser` souhaite lors de l'activation de la règle HTTP Flood Protection ou de la règle de protection Scanner & Probe, et peut être utilisée pour activer la protection contre les mauvais robots grâce à une détection qui fonctionne via une chaîne logique structurée.

Règle AWS WAF

Une règle AWS WAF définit :

- Comment inspecter les requêtes Web HTTP (S)
- La suite à donner à 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.

CloudFront journaux

Cette solution utilise des journaux pour la CloudFront ressource. La règle de protection des scanners et des sondes de cette solution inspecte ces journaux.

Ensemble d'adresses IP

Un ensemble d'adresses IP fournit un ensemble d'adresses IP et de plages d'adresses IP que vous souhaitez utiliser

ensemble dans une déclaration de règle. Les ensembles d'adresses IP sont des ressources AWS.

Analyseur de log Lambda

Cette solution exécute une fonction Lambda invoquée par un événement de création d'objet Amazon Simple Storage Service (Amazon S3). La fonction Lambda lance une inspection des journaux AWS, WAF ou ALB si l'utilisateur le souhaite `yes - AWS Lambda log parser` lors de l'activation de la protection HTTP contre les inondations CloudFront, de la protection du scanner et de la sonde. Elle peut être utilisée pour appliquer la règle de protection contre les robots défectueux grâce à une détection qui fonctionne via une chaîne logique structurée.

Groupes de règles gérés

Les groupes de règles gérés sont des ensembles de ready-to-use règles prédéfinies que les vendeurs d'AWS et d'AWS Marketplace rédigent et mettent à jour pour vous. La tarification d'AWS WAF s'applique à votre utilisation de n'importe quel groupe de règles géré.

type de ressource/point de terminaison

Vous pouvez associer des ressources AWS au Web ACLs pour les protéger. Ces ressources sont les CloudFront ressources ALB, AWS AppSync, Amazon Cognito, AWS App Runner et AWS Verified Access. Actuellement, cette solution est prise en charge par Amazon CloudFront et ALB.

Journaux WAF

Cette solution utilise les journaux générés par AWS WAF pour les ressources associées à l'ACL Web. Les règles HTTP Flood Protection, Scanner & Probe Protection et Activate Bad Bot Protection de cette solution inspectent ces journaux.

WCU

AWS WAF utilise les unités de capacité des listes de contrôle d'accès Web (ACL) (WCUs) pour calculer et contrôler les ressources d'exploitation nécessaires à l'exécution de vos règles, de vos

groupes de règles et du Web. ACLs AWS WAF applique des quotas WCU lorsque vous configurez vos groupes de règles et votre site Web. ACLs WCUs n'affectent pas la façon dont AWS WAF inspecte le trafic Web.

ACL Web

Une ACL Web vous permet de contrôler avec précision les requêtes Web HTTP (S) auxquelles répond votre ressource protégée.

> **Note**
>
> Pour une référence générale des termes AWS, consultez le glossaire AWS.

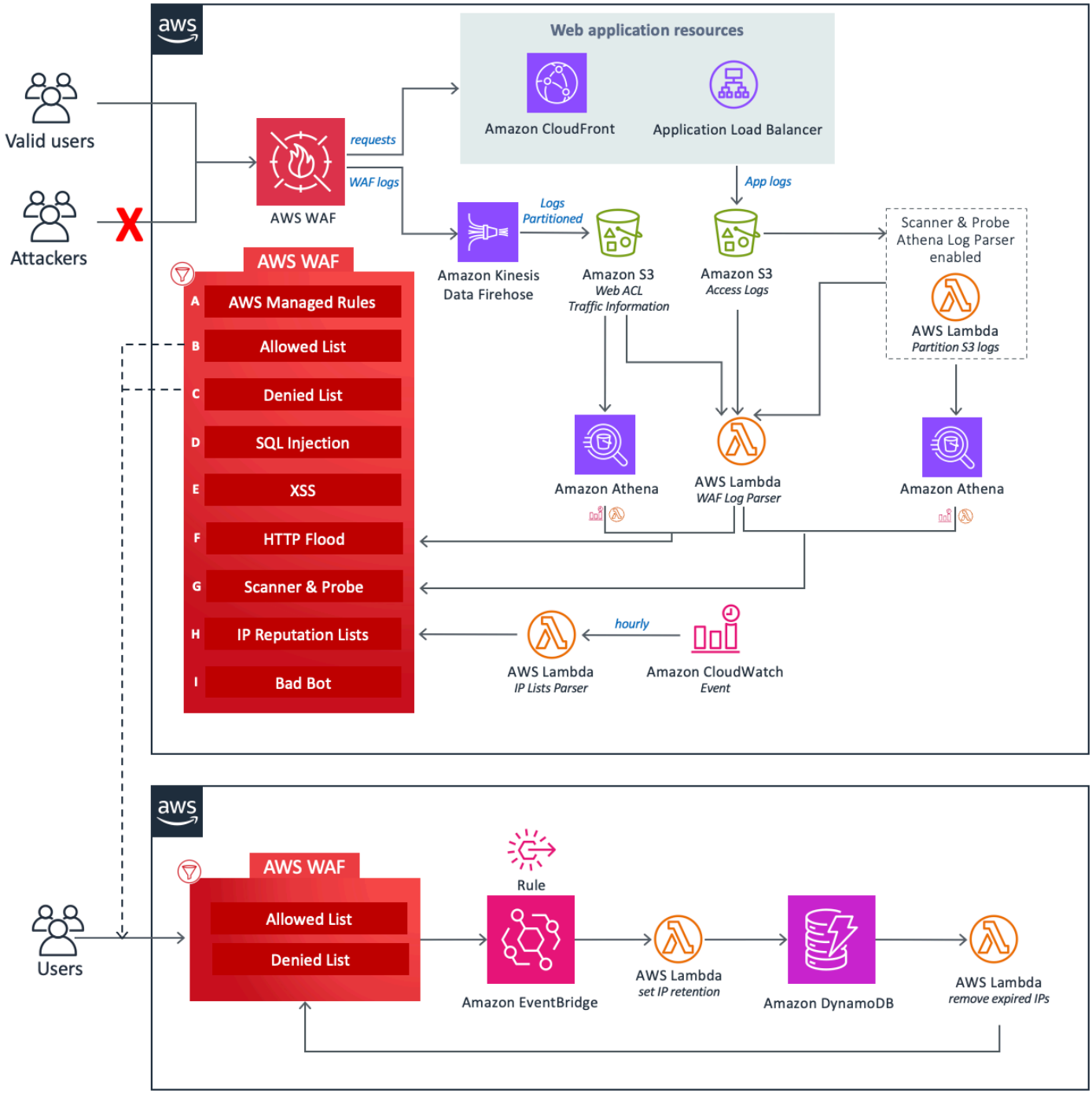
Présentation de l’architecture

Cette section fournit un schéma d'architecture d'implémentation de référence pour les composants déployés avec cette solution.

Diagramme d'architecture

Le déploiement de cette solution avec les paramètres par défaut déploie les composants suivants dans votre compte AWS.

CloudFormation Le modèle déploie AWS WAF et d'autres ressources AWS pour protéger votre application Web contre les attaques courantes.



Au cœur de la conception se trouve une ACL Web AWS WAF, qui sert de point central d'inspection et de décision pour toutes les demandes entrantes adressées à une application Web. Lors de la configuration initiale de la CloudFormation pile, l'utilisateur définit les composants de protection à activer. Chaque composant fonctionne indépendamment et ajoute des règles différentes à l'ACL Web.

Les composants de cette solution peuvent être regroupés dans les domaines de protection suivants.

> **Note**
>
> Les libellés des groupes ne reflètent pas le niveau de priorité des règles WAF.

- AWS Managed Rules (A) : ce composant contient des groupes de règles de réputation IP AWS Managed Rules, des groupes de règles de base et des groupes de règles spécifiques à des cas d'utilisation. Ces groupes de règles protègent contre l'exploitation des vulnérabilités courantes des applications ou contre tout autre trafic indésirable, notamment ceux décrits dans les publications de l'OWASP, sans avoir à écrire vos propres règles.
- Listes d'adresses IP manuelles (B et C) : ces composants créent deux règles AWS WAF. Ces règles vous permettent d'insérer manuellement les adresses IP que vous souhaitez autoriser ou refuser. Vous pouvez configurer la rétention des adresses IP et supprimer les adresses IP expirées sur les ensembles d'adresses IP autorisés ou refusés à l'aide des EventBridge règles Amazon et d'Amazon DynamoDB. Pour plus d'informations, reportez-vous à Configurer la rétention des adresses IP sur les ensembles d'adresses IP AWS WAF autorisés et refusés.
- Injection SQL (D) et XSS (E) : ces composants configurent deux règles AWS WAF conçues pour protéger contre les modèles courants d'injection SQL ou de script intersite (XSS) dans l'URI, la chaîne de requête ou le corps d'une demande.
- HTTP Flood (F) - Ce composant protège contre les attaques consistant en un grand nombre de requêtes provenant d'une adresse IP particulière, telles qu'une attaque de couche Web DDo S ou une tentative de connexion par force brute. Avec cette règle, vous définissez un quota qui définit le nombre maximum de demandes entrantes autorisées à partir d'une seule adresse IP dans un délai de cinq minutes par défaut (configurable avec le paramètre Athena Query Run Time Schedule). Une fois ce seuil dépassé, les demandes supplémentaires provenant de l'adresse IP sont temporairement bloquées. Vous pouvez implémenter cette règle en utilisant une règle basée sur le débit AWS WAF ou en traitant les journaux AWS WAF à l'aide d'une fonction Lambda ou d'une requête Athena. Pour plus d'informations sur les compromis liés aux options d'atténuation des inondations HTTP, reportez-vous à la section Options de l'analyseur de log.
- Scanner et sonde (G) - Ce composant analyse les journaux d'accès aux applications à la recherche de comportements suspects, tels qu'un nombre anormal d'erreurs générées par une origine. Il bloque ensuite ces adresses IP sources suspectes pendant une période définie par le client. Vous pouvez implémenter cette règle à l'aide d'une fonction Lambda ou d'une requête Athena. Pour

plus d'informations sur les compromis liés aux options d'atténuation du scanner et de la sonde, reportez-vous à la section Options de l'analyseur de log.

- Listes de réputation IP (H) - Ce composant est la fonction `IP Lists Parser` Lambda qui vérifie toutes les heures les listes de réputation IP tierces pour détecter les nouvelles plages à bloquer. Ces listes incluent les listes Do't Route Or Peer (DROP) et Extended DROP (EDROP) de Spamhaus, la liste IP des menaces émergentes de Proofpoint et la liste des nœuds de sortie Tor.
- Bad Bot (I) : ce composant améliore la détection des robots malveillants en surveillant les connexions directes à un Application Load Balancer (ALB) ou à Amazon CloudFront, en plus du mécanisme Honeypot. Si un bot contourne le honeypot et tente d'interagir avec ALB CloudFront, le système analyse les modèles de demandes et les journaux pour identifier les activités malveillantes. Lorsqu'un robot malveillant est détecté, son adresse IP est extraite et ajoutée à une liste de blocage AWS WAF pour empêcher tout accès ultérieur. La détection des bots défectueux s'effectue par le biais d'une chaîne logique structurée, garantissant une couverture complète des menaces :
  - Analyseur de journal Lambda HTTP Flood Protection : collecte les bots défectueux à IPs partir des entrées du journal lors de l'analyse des inondations.
  - Analyseur de journal Lambda pour la protection des scanners et des sondes : identifie les robots défectueux à IPs partir des entrées du journal relatives au scanner.
  - Analyseur de journaux Athena pour la protection contre les inondations HTTP : extrait les robots malveillants des journaux IPs Athena, en utilisant des partitions lors de l'exécution des requêtes.
  - Scanner & Probe Protection Athena Log Parser : récupère les robots malveillants des journaux Athena IPs liés au scanner, en utilisant la même stratégie de partitionnement.
  - Détection des failles : si la protection HTTP contre les inondations et la protection contre les scanners et les sondes sont désactivées, le système s'appuie sur l'analyseur Log Lambda, qui enregistre l'activité des robots en fonction des filtres d'étiquettes WAF.

Chacune des trois fonctions Lambda personnalisées de cette solution publie des métriques d'exécution sur. CloudWatch Pour plus d'informations sur ces fonctions Lambda, reportez-vous à la section Détails des composants.

Considérations relatives à la conception d'AWS Well-Architected

Cette solution utilise les meilleures pratiques de l'AWS Well-Architected Framework, qui aide les clients à concevoir et à exploiter des charges de travail fiables, sécurisées, efficaces et rentables dans le cloud.

Cette section décrit comment les principes de conception et les meilleures pratiques du Well-Architected Framework profitent à cette solution.

Excellence opérationnelle

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de l'excellence opérationnelle.

- La solution utilise des métriques pour fournir de l'observabilité CloudWatch à l'infrastructure, aux fonctions Lambda, à Amazon Data Firehose, aux compartiments Amazon S3 et aux autres composants de la solution.
- Nous développons, testons et publions la solution par le biais d'un pipeline d'intégration continue et de livraison continue (CI/CD) AWS. Cela permet aux développeurs d'obtenir des résultats de haute qualité de manière constante.
- Vous pouvez installer la solution à l'aide d'un CloudFormation modèle qui fournit toutes les ressources requises dans votre compte. Pour mettre à jour ou supprimer la solution, il suffit de mettre à jour ou de supprimer le modèle.

Sécurité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de sécurité.

- Toutes les communications interservices utilisent des rôles AWS Identity and Access Management (IAM).
- Tous les rôles utilisés par la solution suivent le principe du moindre privilège d'accès. En d'autres termes, ils ne contiennent que les autorisations minimales requises pour que le service puisse fonctionner correctement.
- Tous les systèmes de stockage de données, y compris les compartiments Amazon S3 et DynamoDB, sont chiffrés au repos.

Fiabilité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de fiabilité.

- La solution utilise les services sans serveur AWS dans la mesure du possible (par exemple, Lambda, Firehose, Amazon S3 et Athena) pour garantir une haute disponibilité et une restauration en cas de panne de service.
- Nous effectuons des tests automatisés sur la solution afin de détecter et de corriger rapidement les erreurs.
- La solution utilise les fonctions Lambda pour le traitement des données. La solution stocke les données dans Amazon S3 et DynamoDB, et elles sont conservées par défaut dans plusieurs zones de disponibilité.

Efficacité des performances

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier de l'efficacité des performances.

- La solution utilise une architecture sans serveur pour garantir une évolutivité et une disponibilité élevées à un coût réduit.
- La solution améliore les performances des bases de données en partitionnant les données et en optimisant les requêtes afin de réduire le volume de numérisation des données et d'obtenir des résultats plus rapides.
- La solution est automatiquement testée et déployée chaque jour. Nos architectes de solutions et nos experts en la matière examinent la solution pour identifier les domaines à expérimenter et à améliorer.

Optimisation des coûts

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier d'optimisation des coûts.

- La solution utilise une architecture sans serveur et les clients ne paient que pour ce qu'ils utilisent.
- La couche de calcul de la solution utilise par défaut Lambda, qui utilise pay-per-use un modèle.
- La base de données et les requêtes Athena sont optimisées pour réduire le volume de numérisation des données, réduisant ainsi les coûts.

Durabilité

Cette section décrit comment nous avons conçu cette solution en utilisant les principes et les meilleures pratiques du pilier du développement durable.

- La solution utilise des services gérés et sans serveur pour minimiser l'impact environnemental des services principaux.
- La conception sans serveur de la solution vise à réduire l'empreinte carbone par rapport à l'empreinte des serveurs sur site fonctionnant en permanence.

Détails de l'architecture

Cette section décrit les composants et les services AWS qui constituent cette solution ainsi que les détails de l'architecture sur la manière dont ces composants fonctionnent ensemble.

Services AWS inclus dans cette solution

Service AWS	Description
AWS WAF	Noyau. Déploie une ACL Web AWS WAF, des groupes de règles AWS Managed Rules, des règles personnalisées et des ensembles d'adresses IP. Effectue des appels à l'API AWS WAF pour bloquer les attaques courantes et sécuriser les applications Web.
Amazon Data Firehose	Noyau. Fournit les journaux AWS WAF aux compartiments Amazon S3.
Amazon S3	Noyau. Stocke les journaux AWS CloudFront, WAF et ALB.
AWS Lambda	Noyau. Déploie plusieurs fonctions Lambda pour prendre en charge les règles personnal isées.
Amazon EventBridge	Noyau. Crée des règles d'événements pour appeler Lambda.
Amazon Athena	Soutenir. Crée des requêtes Athena et des groupes de travail pour prendre en charge l'analyseur de log Athena.
AWS Glue	Soutenir. Crée des bases de données et des tables pour prendre en charge l'analyseur de log Athena.

Service AWS	Description
Amazon SNS	Soutenir. Envoie des notifications par e-mail à Amazon Simple Notification Service (Amazon SNS) pour soutenir la rétention des adresses IP sur les listes autorisées et refusées.
AWS Systems Manager	Soutenir. Assure la surveillance des ressources au niveau de l'application et la visualisation des opérations sur les ressources et des données de coûts.

Options de l'analyseur de journaux

Comme décrit dans la présentation de l'architecture, il existe trois options pour gérer le flux HTTP et les protections des scanners et des sondes. Les sections suivantes expliquent chacune de ces options plus en détail.

Règle basée sur le taux AWS WAF

Des règles basées sur le débit sont disponibles pour la protection HTTP contre les inondations. Par défaut, une règle basée sur le débit agrège et limite les demandes en fonction de l'adresse IP de la demande. Cette solution vous permet de spécifier le nombre de requêtes Web autorisées par l'adresse IP d'un client au cours d'une période de cinq minutes, mise à jour en continu. Si une adresse IP dépasse le quota configuré, AWS WAF bloque les nouvelles demandes bloquées jusqu'à ce que le taux de demandes soit inférieur au quota configuré.

Nous vous recommandons de sélectionner l'option de règle basée sur le taux si le quota de demandes est supérieur à 2 000 demandes par cinq minutes et que vous n'avez pas besoin de mettre en œuvre de personnalisations. Par exemple, vous ne tenez pas compte de l'accès statique aux ressources lorsque vous comptez les demandes.

Vous pouvez également configurer la règle pour utiliser diverses autres clés d'agrégation et combinaisons de touches. Pour plus d'informations, consultez la section Options et clés d'agrégation.

Analyseur de journaux Amazon Athena

Les paramètres du modèle HTTP Flood Protection et Scanner & Probe Protection fournissent l'option Athena log parser. Lorsqu'elle est activée, CloudFormation fournit une requête Athena et une fonction Lambda planifiée chargées d'orchestrer l'exécution d'Athena, de traiter la sortie des résultats et de mettre à jour AWS WAF. Cette fonction Lambda est invoquée par un CloudWatch événement configuré pour s'exécuter toutes les cinq minutes. Ceci est configurable avec le paramètre Athena Query Run Time Schedule.

Nous vous recommandons de sélectionner cette option lorsque vous ne pouvez pas utiliser les règles basées sur le débit AWS WAF et que vous connaissez le langage SQL pour implémenter des personnalisations. Pour plus d'informations sur la modification de la requête par défaut, consultez la section Afficher les requêtes Amazon Athena.

La protection HTTP contre les inondations est basée sur le traitement des journaux d'accès AWS WAF et utilise les fichiers journaux WAF. Le type de journal d'accès WAF présente un temps de latence plus faible, que vous pouvez utiliser pour identifier plus rapidement les origines des inondations HTTP par rapport au CloudFront délai de livraison du journal ALB. Cependant, vous devez sélectionner le type de journal CloudFront ou ALB dans le paramètre du modèle Activate Scanner & Probe Protection pour recevoir les codes d'état des réponses.

> **Note**
>
> Si un robot malveillant contourne le honeypot et interagit directement avec ALB, le système détecte un comportement malveillant par le biais d'une analyse des journaux CloudFront, sauf si HTTP Flood Protection et Scanner & Probe Protection n'utilisent pas l'analyseur de journaux Lambda.

Analyseur de journaux AWS Lambda

Les paramètres du modèle HTTP Flood Protection et Scanner & Probe Protection fournissent l'option AWS Lambda Log Parser. Utilisez l'analyseur de journaux Lambda uniquement lorsque la règle basée sur le débit AWS WAF et les options de l'analyseur de journaux Amazon Athena ne sont pas disponibles. L'une des limites connues de cette option est que les informations sont traitées dans le contexte du fichier en cours de traitement. Par exemple, une adresse IP peut générer plus de demandes ou d'erreurs que le quota défini, mais comme ces informations sont réparties dans différents fichiers, chaque fichier ne stocke pas suffisamment de données pour dépasser le quota.

> **Note**
>
> En outre, si un robot malveillant contourne le honeypot et interagit directement avec ALB CloudFront, la détection repose sur l'option d'analyseur de journal choisie pour identifier et bloquer efficacement les activités malveillantes.

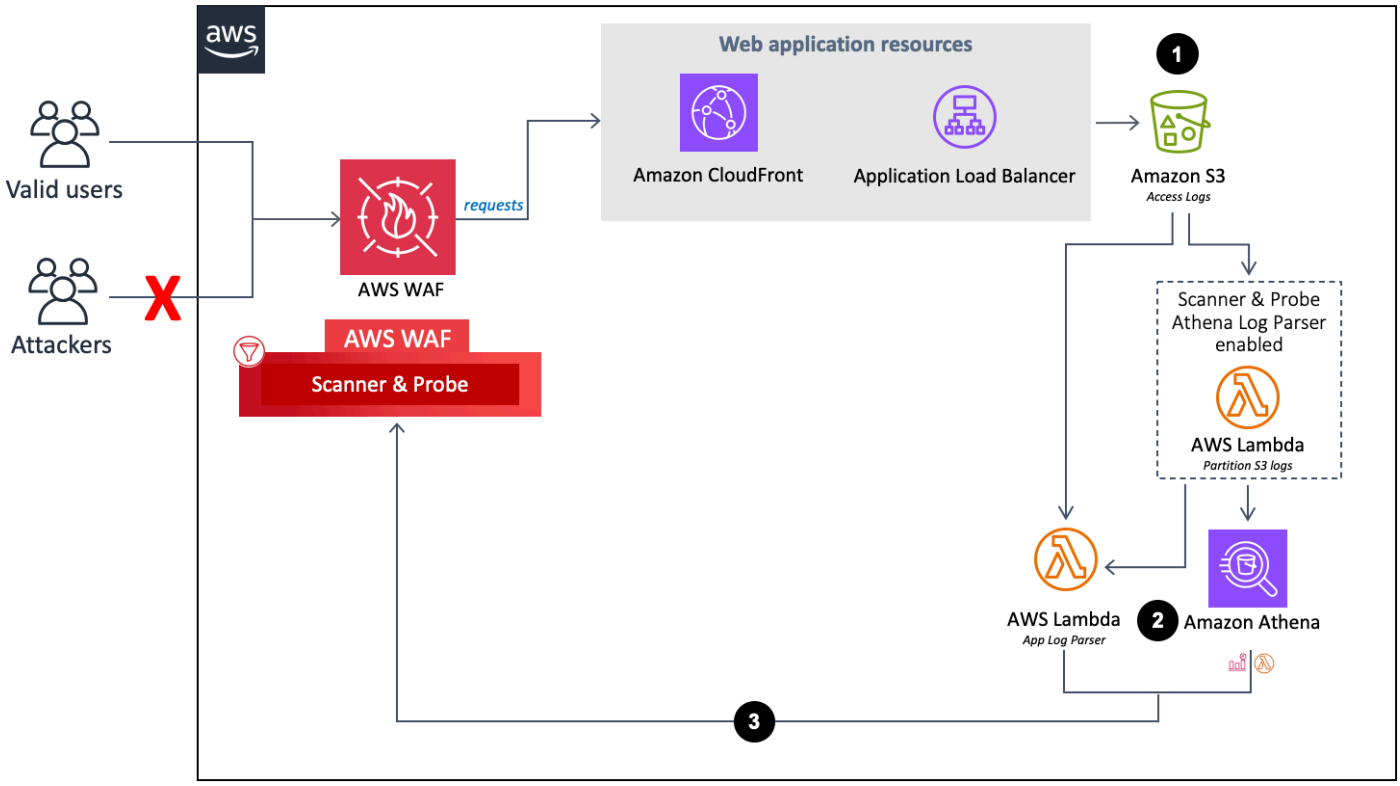
Détails des composants

Comme décrit dans le schéma d'architecture, quatre des composants de cette solution utilisent des automatisations pour inspecter les adresses IP et les ajouter à la liste de blocage d'AWS WAF. Les sections suivantes expliquent chacun de ces composants de manière plus détaillée.

Log parser - Application

L'analyseur du journal des applications permet de se protéger contre les scanners et les sondes.

Flux de l'analyseur du journal des applications.



1. Lorsqu' CloudFront un ALB reçoit des demandes au nom de votre application Web, il envoie des journaux d'accès à un compartiment Amazon S3.

   a. (Facultatif) Si vous sélectionnez `Yes - Amazon Athena log parser` comme paramètres du modèle Activate HTTP Flood Protection et Activate Scanner & Probe Protection, une fonction Lambda déplace les journaux d'accès de leur dossier d'origine *`<customer-bucket>`* `/AWSLogs` vers un dossier nouvellement *`<customer-bucket>`* `/AWSLogs-partitioned/` *`<optional-prefix>`* `/year=` *`<YYYY>`* `/month=` *`<MM>`* `/day=` *`<DD>`* `/hour=` *`<HH>`* partitionné/ à leur arrivée dans Amazon S3.

   b. (Facultatif) Si vous sélectionnez `yes` le paramètre Conserver les données dans l'emplacement S3 d'origine, les journaux restent dans leur emplacement d'origine et sont copiés dans leur dossier partitionné, dupliquant ainsi votre stockage de journaux.

   > **Note**
   >
   > Pour l'analyseur de journaux Athena, cette solution partitionne uniquement les nouveaux journaux qui arrivent dans votre compartiment Amazon S3 après le déploiement de cette solution. Si vous souhaitez partitionner des journaux existants, vous devez les charger manuellement sur Amazon S3 après avoir déployé cette solution.

2. En fonction de votre sélection pour les paramètres du modèle Activate HTTP Flood Protection et Activate Scanner & Probe Protection, cette solution traite les journaux en utilisant l'une des méthodes suivantes :

   a. Lambda - Chaque fois qu'un nouveau journal d'accès est stocké dans le compartiment Amazon S3, la fonction `Log Parser` Lambda est lancée.

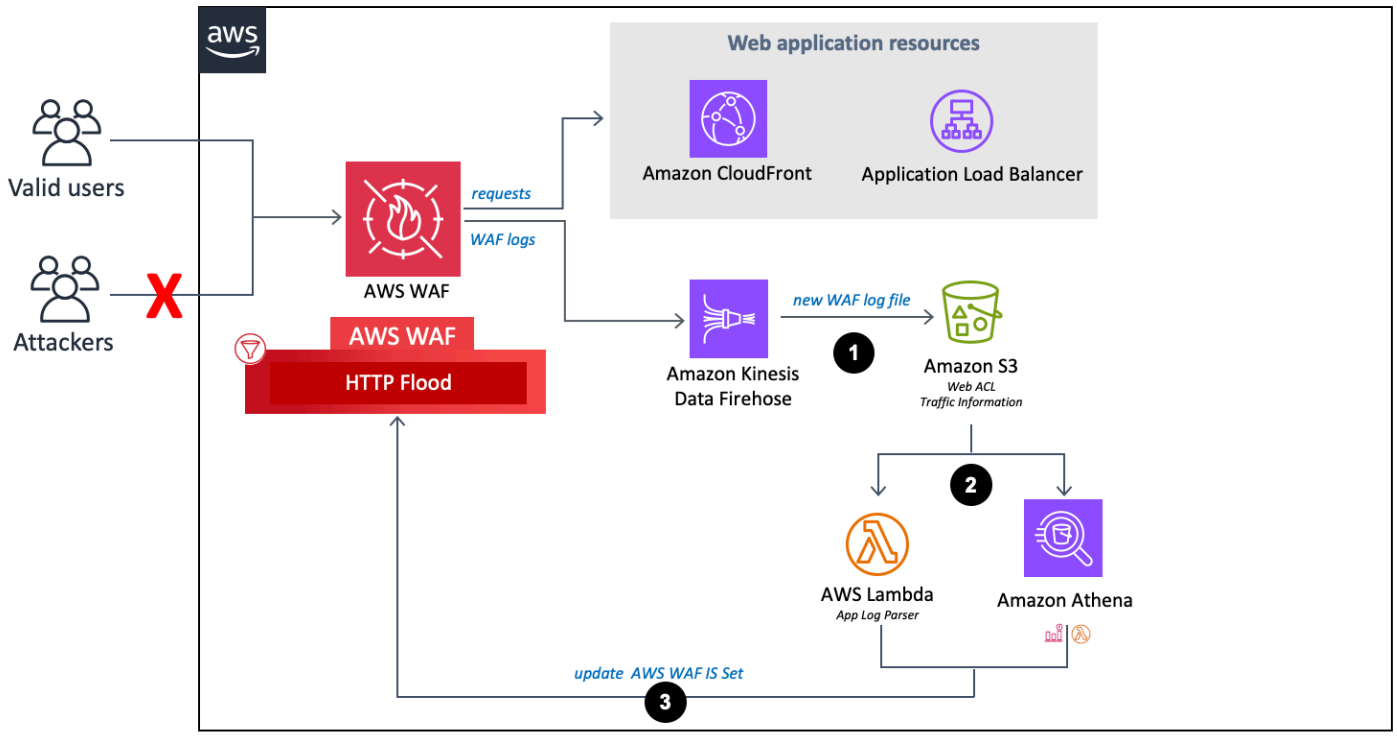
   b. Athena - Par défaut, toutes les cinq minutes, la requête Athena de Scanner & Probe Protection est exécutée et le résultat est envoyé vers AWS WAF. Ce processus est initié par un CloudWatch événement qui lance la fonction Lambda chargée d'exécuter la requête Athena et envoie le résultat dans AWS WAF.

3. La solution analyse les données du journal pour identifier les adresses IP qui ont généré plus d'erreurs que le quota défini. La solution met ensuite à jour une condition d'ensemble d'adresses IP AWS WAF afin de bloquer ces adresses IP pendant une période définie par le client.

Analyseur de journaux - AWS WAF

Si vous sélectionnez `yes - AWS Lambda log parser` ou `yes - Amazon Athena log parser` pour Activer la protection HTTP contre les inondations, cette solution fournit les composants suivants, qui analysent les journaux AWS WAF afin d'identifier et de bloquer les origines qui inondent le point de terminaison avec un taux de demandes supérieur au quota que vous avez défini.

Flux de l'analyseur de journaux AWS WAF.



1. Lorsqu'AWS WAF reçoit des journaux d'accès, il les envoie à un point de terminaison Firehose. Firehose envoie ensuite les journaux dans un compartiment partitionné dans Amazon S3 nommé *<customer-bucket>* /AWSLogs/ *<optional-prefix>* /year= *<YYYY>* /month= *<MM>* / day= *<DD>* /hour= *<HH>* /
2. En fonction de votre sélection pour les paramètres du modèle Activate HTTP Flood Protection et Activate Scanner & Probe Protection, cette solution traite les journaux en utilisant l'une des méthodes suivantes :
   a. Lambda : chaque fois qu'un nouveau journal d'accès est stocké dans le compartiment Amazon S3, la fonction `Log Parser` Lambda est lancée.
   b. Athena : Par défaut, toutes les cinq minutes, la requête Athena du scanner et de la sonde est exécutée et le résultat est transféré vers AWS WAF. Ce processus est initié par un CloudWatch

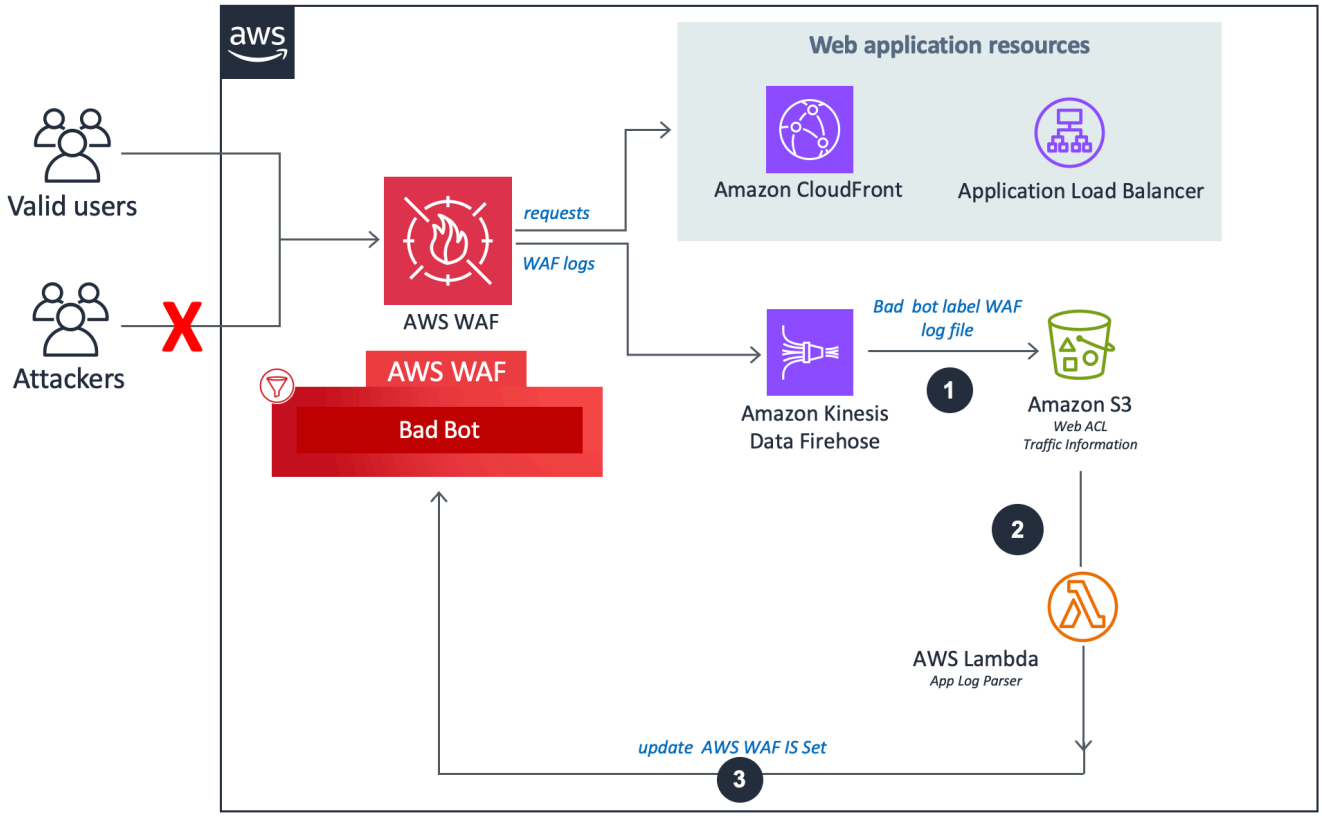
événement Amazon, qui lance ensuite la fonction Lambda chargée d'exécuter la requête Amazon Athena et envoie le résultat dans AWS WAF.

3. La solution analyse les données du journal pour identifier les adresses IP qui ont envoyé plus de demandes que le quota défini. La solution met ensuite à jour une condition d'ensemble d'adresses IP AWS WAF afin de bloquer ces adresses IP pendant une période définie par le client.

Log parser - Mauvais robot

L'analyseur de log Bad bot inspecte les requêtes adressées au point de terminaison Honeypot pour en extraire l'adresse IP source.

Le flux de l'analyseur de journal des bots est incorrect.



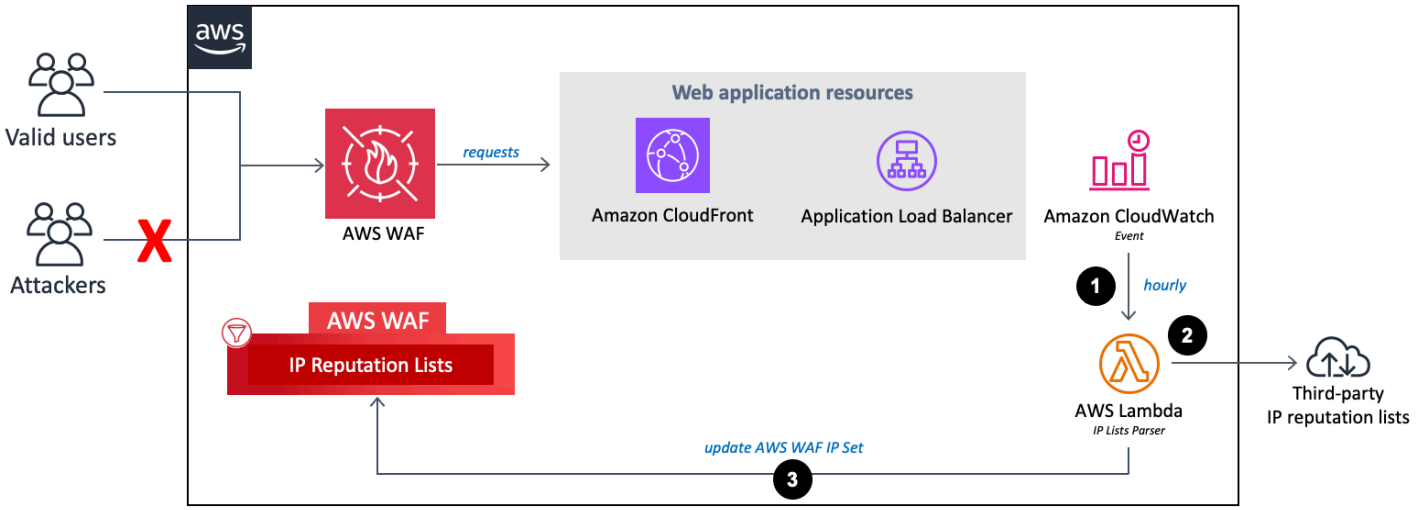
1. S'il `Bad Bot Protection` est activé et que les fonctionnalités de protection contre les inondations HTTP et de protection contre les scanners et les sondes sont désactivées : le système utilisera l'analyseur Log Lambda, qui enregistre uniquement les mauvaises requêtes de bot sur la base des filtres d'étiquettes WAF.

2. La fonction Lambda intercepte et inspecte les en-têtes de requête pour extraire l'adresse IP de la source qui a accédé au point de terminaison du trap.
3. La solution analyse les données du journal pour identifier les adresses IP qui ont envoyé plus de demandes que le quota défini. La solution met ensuite à jour une condition d'ensemble d'adresses IP AWS WAF afin de bloquer ces adresses IP pendant une période définie par le client.

Analyseur de listes IP

La fonction `IP Lists Parser` Lambda permet de se protéger contre les attaquants connus identifiés dans les listes de réputation IP tierces.

La réputation IP répertorie les flux d'analyseurs.



1. Un CloudWatch événement Amazon horaire appelle la fonction `IP Lists Parser` Lambda.
2. La fonction Lambda collecte et analyse les données provenant de trois sources :
   - Listes DROP et EDROP de Spamhaus
   - Liste IP des menaces émergentes de Proofpoint
   - Liste des nœuds de sortie de Tor
3. La fonction Lambda met à jour la liste de blocage AWS WAF avec les adresses IP actuelles.

Planifiez votre déploiement

Cette section décrit les coûts, la sécurité, les quotas et les autres considérations à prendre en compte avant de déployer la solution.

Régions AWS prises en charge

Selon les valeurs des paramètres d'entrée du modèle que vous définissez, cette solution nécessite différentes ressources. Ces ressources (répertoriées dans le tableau suivant) ne sont peut-être pas disponibles dans toutes les régions AWS. Par conséquent, vous devez lancer cette solution dans une région AWS où ces services sont disponibles. Pour connaître la disponibilité la plus récente des services AWS par région, consultez la liste des services régionaux AWS.

	ACL Web AWS WAF	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Type de point de terminaison				
CloudFront	✓			
Application Load Balancer (ALB)	✓			
Activer la protection HTTP contre les inondations				
oui - Analyseur de journaux AWS Lambda				✓
oui - Analyseur de journaux Amazon Athena		✓	✓	✓

	ACL Web AWS WAF	AWS Glue	Amazon Athena	Amazon Kinesis Data Firehose
Activer la protection du scanner et de la sonde				
oui - Analyseur de journaux Amazon Athena		✓	✓	

> **Note**
>
> Si vous `CloudFront` le choisissez comme point de terminaison, vous devez déployer la solution dans la région USA Est (Virginie du Nord) (`us-east-1`).

Cost

Vous êtes responsable du coût des services AWS utilisés lors de l'exécution de la solution Security Automations for AWS WAF. Le coût total de fonctionnement de cette solution dépend de la protection activée et de la quantité de données ingérées, stockées et traitées.

Nous vous recommandons de créer un budget via AWS Cost Explorer pour vous aider à gérer les coûts. Pour plus de détails, consultez la page Web de tarification de chaque service AWS que vous avez utilisé dans cette solution.

Les tableaux suivants présentent des exemples de ventilation des coûts liés à l'exécution de cette solution dans la région de l'est des États-Unis (Virginie du Nord) (à l'exception du niveau gratuit d'AWS). Les prix sont susceptibles d’être modifiés.

Exemple 1 : activation de la protection des listes de réputation, de la protection contre les robots malveillants, de l'analyseur de journaux AWS Lambda pour la protection contre les inondations HTTP et de la protection contre les scanners et les sondes

Service AWS	Dimensions/mois	Coût [USD]
Amazon Data Firehose	100 Go	~2,90 $
Amazon S3	100 Go	~2,30 $
AWS Lambda	128 Mo : 3 fonctions, 1 million d'appels et durée moyenne de 500 millisecondes par exécution Lambda 512 Mo : 2 fonctions, 1 million d'appels et durée moyenne de 500 millisecondes par exécution Lambda	~5,40 $
ACL Web AWS WAF	1	5,00$
Règle AWS WAF	4	4,00$
Requête AWS WAF	1 M	0,60$
Total		~20,60 $ par mois

Exemple 2 : activer la protection des listes de réputation, la protection contre les robots malveillants, l'analyseur de journal Amazon Athena pour la protection contre les inondations HTTP et la protection contre les scanners et les sondes

Service AWS	Dimensions/mois	Coût [USD]
Amazon Data Firehose	100 Go	~2,90 $
Amazon S3	100 Go	~2,30 $
AWS Lambda	128 Mo : 3 fonctions, 1 million d'appels et durée moyenne de 500 millisecondes par exécution Lambda	~1,26 $

Service AWS	Dimensions/mois	Coût [USD]
	512 Mo : 2 fonctions, 7 560 appels et une durée moyenne de 500 millisecondes par exécution Lambda	
Amazon Athena	1,2 million de visites CloudFront d'objets ou 1,2 million de requêtes ALB par jour, ce qui génère un enregistrement de journal d'environ 500 octets par accès ou demande	~4,32 $
ACL Web AWS WAF	1	5,00$
Règle AWS WAF	4	4,00$
Requête AWS WAF	1 M	0,60$
Total		~20,38 $ par mois

Exemple 3 : activer la rétention des adresses IP pour les ensembles d'adresses IP autorisés et refusés

Service AWS	Dimensions/mois	Coût [USD]
Amazon DynamoDB	1 000 écritures et 1 Mo de stockage de données	~0,00 $
AWS Lambda	128 Mo : 1 fonction, 2 000 appels et durée moyenne de 500 millisecondes par exécution Lambda 512 Mo : 1 fonction, 2 000 appels et durée moyenne	~0,01 $

Service AWS	Dimensions/mois	Coût [USD]
	de 500 millisecondes par exécution Lambda	
Amazon CloudWatch	Événements 2K	~0,00 $
ACL Web AWS WAF	1	5,00$
Règle AWS WAF	2	2,00$
Requête WAF WAS	1 M	0,60$
Total		~7,61 $ par mois

Estimation du coût des CloudWatch grumes

Certains services AWS utilisés dans cette solution, tels que Lambda, génèrent des CloudWatch journaux. Ces journaux sont payants. Nous vous recommandons de supprimer ou d'archiver les journaux pour réduire les coûts. Pour plus de détails sur l'archivage des journaux, reportez-vous à la section Exportation des données des CloudWatch journaux vers Amazon S3 dans le guide de l'utilisateur Amazon Logs.

Si vous choisissez d'utiliser l'analyseur de journaux Athena lors de l'installation, cette solution planifie l'exécution d'une requête par rapport à l'AWS WAF ou aux journaux d'accès aux applications de vos compartiments Amazon S3 tels que configurés. Vous êtes facturé en fonction de la quantité de données numérisées par chaque requête. La solution applique le partitionnement aux journaux et aux requêtes afin de minimiser les coûts. Par défaut, la solution déplace les journaux d'accès aux applications de leur emplacement Amazon S3 d'origine vers une structure de dossiers partitionnée. Vous pouvez également conserver l'original, mais le stockage de journaux dupliqués vous sera facturé. Cette solution utilise des groupes de travail pour segmenter les charges de travail, et vous pouvez configurer les deux pour gérer l'accès aux requêtes et les coûts. Reportez-vous à la section Estimation des coûts d'Athéna pour un exemple de calcul d'estimation des coûts. Pour plus d'informations, consultez la section Tarification d'Amazon Athena.

Estimation des coûts d'Athéna

Si vous utilisez l'option Athena log parser lors de l'exécution des règles HTTP Flood Protection, Scanner & Probe Protection ou Bad Bot Protection, l'utilisation d'Athena vous sera facturée. Par

défaut, chaque requête Athena est exécutée toutes les cinq minutes et analyse les données des quatre dernières heures. La solution applique le partitionnement aux journaux et aux requêtes Athena afin de minimiser les coûts. Vous pouvez configurer le nombre d'heures de données analysées par une requête en modifiant la valeur du paramètre du modèle WAF Block Period. Cependant, l'augmentation de la quantité de données numérisées augmentera probablement le coût d'Athena.

> **Tip**
>
> Voici un exemple de calcul du coût CloudFront des journaux :
> En moyenne, chaque CloudFront accès peut générer environ 500 octets de données.
> Si 1,2 million d' CloudFront objets sont touchés par jour, il y aura 200 000 accès (1,2 M/6) par quatre heures, en supposant que les données sont ingérées à un rythme constant. Tenez compte de vos modèles de trafic réels lorsque vous calculez vos coûts.
> `[500 bytes of data] * [200K hits per four hours] = [an average 100 MB (0.0001TB) data scanned per query]`
> Athena facture 5$ par To de données numérisées.
> `[0.0001 TB] * [$5] = [$0.0005 per query scan]`
> La requête Athena s'exécute toutes les cinq minutes, soit 12 exécutions par heure.
> `[12 runs] * [24 hours] = [288 runs per day]`
> `[$0.0005 per query scan] * [288 runs per day] * [30 days] = [$4.32 per month]`
> Les coûts réels varient en fonction des modèles de trafic de votre application. Pour plus d'informations, consultez la section Tarification d'Amazon Athena.

Sécurité

Lorsque vous créez des systèmes sur l'infrastructure AWS, les responsabilités en matière de sécurité sont partagées entre vous et AWS. Ce modèle de responsabilité partagée réduit votre charge opérationnelle car AWS exploite, gère et contrôle les composants, notamment le système d'exploitation hôte, la couche de virtualisation et la sécurité physique des installations dans lesquelles les services fonctionnent. Pour plus d'informations sur la sécurité AWS, rendez-vous sur AWS Cloud Security.

Rôles IAM

Avec les rôles IAM, vous pouvez attribuer des accès, des politiques et des autorisations granulaires aux services et aux utilisateurs sur le cloud AWS. Cette solution crée des rôles IAM dotés de

privilèges minimaux, et ces rôles accordent aux ressources de la solution les autorisations nécessaires.

Données

Toutes les données stockées dans les compartiments Amazon S3 et les tables DynamoDB sont cryptées au repos. Les données en transit avec Firehose sont également cryptées.

Capacités de protection

Les applications Web sont vulnérables à diverses attaques. Ces attaques incluent des requêtes spécialement conçues pour exploiter une vulnérabilité ou prendre le contrôle d'un serveur, des attaques volumétriques conçues pour détruire un site Web ou des robots malveillants et des scrapers programmés pour récupérer et voler du contenu Web.

Cette solution permet CloudFormation de configurer les règles AWS WAF, y compris les groupes de règles AWS Managed Rules et les règles personnalisées, afin de bloquer les attaques courantes suivantes :

- Règles gérées par AWS : ce service géré fournit une protection contre les vulnérabilités courantes des applications ou contre tout autre trafic indésirable. Cette solution inclut des groupes de règles de réputation IP gérés par AWS, des groupes de règles de base gérés par AWS et des groupes de règles spécifiques à des cas d'utilisation gérés par AWS. Vous avez la possibilité de sélectionner un ou plusieurs groupes de règles pour votre ACL Web, dans la limite du quota d'unités de capacité maximale de l'ACL Web (WCU).
- Injection SQL : les attaquants insèrent du code SQL malveillant dans des requêtes Web pour extraire des données de votre base de données. Nous avons conçu cette solution pour bloquer les requêtes Web contenant du code SQL potentiellement malveillant.
- XSS - Les attaquants utilisent les vulnérabilités d'un site Web bénin pour injecter des scripts malveillants de site client dans le navigateur Web d'un utilisateur légitime. Nous l'avons conçu pour inspecter les éléments fréquemment explorés des demandes entrantes afin d'identifier et de bloquer les attaques XSS.
- Inondations HTTP : les serveurs Web et autres ressources dorsales sont exposés au risque d'attaques DDo S, telles que les inondations HTTP. Cette solution invoque automatiquement une règle basée sur le taux lorsque les demandes Web d'un client dépassent un quota configurable. Vous pouvez également appliquer ce quota en traitant les journaux AWS WAF à l'aide d'une fonction Lambda ou d'une requête Athena.

- Analyseurs et sondes : des sources malveillantes analysent et analysent les applications Web connectées à Internet pour détecter les vulnérabilités, en envoyant une série de requêtes qui génèrent des codes d'erreur HTTP 4xx. Vous pouvez utiliser cet historique pour identifier et bloquer les adresses IP sources malveillantes. Cette solution crée une fonction Lambda CloudFront ou une requête Athena qui analyse automatiquement les journaux d'accès ALB, compte le nombre de demandes erronées provenant d'adresses IP sources uniques par minute et met à jour AWS WAF pour bloquer les analyses ultérieures provenant d'adresses ayant atteint le quota d'erreur défini.
- Origines connues des attaquants (listes de réputation IP) - De nombreuses entreprises tiennent à jour des listes de réputation d'adresses IP exploitées par des attaquants connus, tels que des spammeurs, des distributeurs de logiciels malveillants et des botnets. Cette solution exploite les informations contenues dans ces listes de réputation pour vous aider à bloquer les demandes provenant d'adresses IP malveillantes. En outre, cette solution bloque les attaquants identifiés par des groupes de règles de réputation IP sur la base des informations internes d'Amazon sur les menaces.
- Bots et scrapers - Les opérateurs d'applications Web accessibles au public doivent être sûrs que les clients accédant à leur contenu s'identifient correctement et qu'ils utilisent les services comme prévu. Cependant, certains clients automatisés, tels que les scrapeurs de contenu ou les robots malveillants, se présentent sous un faux jour pour contourner les restrictions. Cette solution vous aide à identifier et à bloquer les robots malveillants et les scrapers.

Quotas

Les quotas de service, également appelés limites, représentent le nombre maximal de ressources ou d'opérations de service pour votre compte AWS.

Quotas pour les services AWS dans cette solution

Assurez-vous de disposer d'un quota suffisant pour chacun des services mis en œuvre dans cette solution. Pour plus d'informations, consultez la section Quotas de service AWS. Pour voir les quotas de service pour tous les services AWS dans la documentation sans changer de page, consultez plutôt les informations de la page Points de terminaison et quotas du service dans le PDF.

Quotas AWS WAF

AWS WAF peut bloquer un maximum de 10 000 plages d'adresses IP en notation CIDR (Classless Inter-Domain Routing) par condition de correspondance IP. Chaque liste créée par cette solution est soumise à ce quota. Pour plus d'informations, consultez la section Quotas AWS WAF. À partir de la

version 3.0, cette solution crée deux ensembles d'adresses IP à associer à chaque règle, un pour IPv4 et un pour IPv6.

AWS WAF autorise un maximum d'une demande par seconde, par compte, par région AWS pour les appels d'API destinés à une personne `Create` ou `Update` à une `Put` action. Si vous effectuez ces appels d'API en dehors de la solution, il se peut que vous rencontriez un problème de limitation de l'API. Pour éviter ce problème, nous vous recommandons d'éviter d'exécuter d'autres applications qui effectuent ces appels d'API dans le même compte et dans la même région où cette solution est déployée.

Considérations relatives au déploiement

Les sections suivantes présentent les contraintes et les considérations relatives à la mise en œuvre de cette solution.

Règles AWS WAF

L'ACL Web généré par cette solution est conçue pour offrir une protection complète aux applications Web. La solution fournit un ensemble de règles gérées par AWS et de règles personnalisées que vous pouvez ajouter à l'ACL Web. Pour inclure une règle, choisissez `yes` les paramètres appropriés lors du lancement de la CloudFormation pile. Voir l'étape 1. Lancez la pile pour la liste des paramètres.

> **Note**
>
> La out-of-box solution ne prend pas en charge AWS Firewall Manager. Si vous souhaitez utiliser les règles de Firewall Manager, nous vous recommandons d'appliquer des personnalisations à son code source.

Journalisation du trafic Web ACL

Si vous créez la pile dans une région AWS autre que l'est des États-Unis (Virginie du Nord) et que vous définissez le point de terminaison comme tel`CloudFront`, vous devez définir Activate HTTP Flood Protection sur no ou`yes - AWS WAF rate based rule`.

Les deux autres options (`yes - AWS Lambda log parser`et`yes - Amazon Athena log parser`) nécessitent l'activation des journaux AWS WAF sur une ACL Web qui s'exécute dans tous les emplacements périphériques AWS, ce qui n'est pas pris en charge en dehors de l'est des États-

Unis (Virginie du Nord). Pour plus d'informations sur la journalisation du trafic ACL Web, consultez le guide du développeur AWS WAF.

Gestion des composants de demande surdimensionnés

AWS WAF ne prend pas en charge l'inspection du contenu surdimensionné pour détecter le corps, les en-têtes ou les cookies du composant de requête Web. Lorsque vous rédigez une instruction de règle qui inspecte l'un de ces types de composants de demande, vous pouvez choisir l'une des options suivantes pour indiquer à AWS WAF ce qu'il doit faire avec ces demandes :

- `yes`(continue) - Inspectez le composant de demande normalement conformément aux critères d'inspection des règles. AWS WAF inspecte le contenu du composant de demande qui respecte les limites de taille. Il s'agit de l'option par défaut utilisée dans la solution.
- `yes - MATCH` - Traiter la demande Web comme correspondant à l'instruction de règle. AWS WAF applique l'action de règle à la demande sans l'évaluer par rapport aux critères d'inspection de la règle. Pour une règle comportant une `Block` action, cela bloque la demande avec le composant surdimensionné.
- `yes - 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.

Pour plus d'informations, reportez-vous à la section Gestion des composants de requêtes Web surdimensionnés dans AWS WAF.

Déploiements de solutions multiples

Vous pouvez déployer la solution plusieurs fois dans le même compte et dans la même région. Vous devez utiliser un nom de CloudFormation pile et un nom de compartiment Amazon S3 uniques pour chaque déploiement. Chaque déploiement unique entraîne des frais supplémentaires et est soumis aux quotas AWS WAF par compte et par région.

Autorisations de rôle minimales pour le déploiement (facultatif)

Les clients peuvent créer manuellement un rôle IAM avec les autorisations minimales requises pour le déploiement :

- Autorisations WAF

```
        {
            "Effect": "Allow",
            "Action": [
                "wafv2:CreateWebACL",
                "wafv2:UpdateWebACL",
                "wafv2:DeleteWebACL",
                "wafv2:GetWebACL",
                "wafv2:ListWebACLs",
                "wafv2:CreateIPSet",
                "wafv2:UpdateIPSet",
                "wafv2:DeleteIPSet",
                "wafv2:GetIPSet",
                "wafv2:AssociateWebACL",
                "wafv2:DisassociateWebACL",
                "wafv2:PutLoggingConfiguration",
                "wafv2:DeleteLoggingConfiguration",
                "wafv2:ListWebACLs",
                "wafv2:ListIPSets",
                "wafv2:ListTagsForResource"
            ],
            "Resource": [
                "arn:aws:wafv2:*:*:regional/webacl/*",
                "arn:aws:wafv2:*:*:regional/ipset/*",
                "arn:aws:wafv2:*:*:global/webacl/*",
                "arn:aws:wafv2:*:*:global/ipset/*"
            ]
        }
```

- Autorisations Lambda

```
        {
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:InvokeFunction",
                "lambda:UpdateFunctionCode",
                "lambda:UpdateFunctionConfiguration",
                "lambda:AddPermission",
                "lambda:RemovePermission"
            ],
```

```
            "Resource": "arn:aws:lambda:*:*:function:*"
        }
```

- Autorisations Firehose

```
        {
            "Effect": "Allow",
            "Action": [
                "firehose:CreateDeliveryStream",
                "firehose:DeleteDeliveryStream",
                "firehose:DescribeDeliveryStream",
                "firehose:StartDeliveryStreamEncryption",
                "firehose:StopDeliveryStreamEncryption",
                "firehose:UpdateDestination"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/*"
        }
```

- Autorisations S3

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucketPolicy",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:GetObject",
                "s3:PutBucketAcl",
                "s3:PutBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutBucketVersioning",
                "s3:PutEncryptionConfiguration",
                "s3:PutObject",
                "s3:PutBucketTagging",
                "s3:PutLifecycleConfiguration",
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
```

```
                "s3:ListMultipartUploadParts",
                "s3:PutBucketLogging",
                "s3:GetBucketLogging"
            ],
            "Resource": "arn:aws:s3:::*"
        }
```

- Autorisations d'Athéna

```
        {
            "Effect": "Allow",
            "Action": [
                "athena:CreateWorkGroup",
                "athena:DeleteWorkGroup",
                "athena:GetWorkGroup",
                "athena:UpdateWorkGroup",
                "athena:StartQueryExecution",
                "athena:GetQueryExecution",
                "athena:GetQueryResults",
                "athena:StopQueryExecution"
            ],
            "Resource": "arn:aws:athena:*:*:workgroup/WAF*"
        }
```

- Autorisations Glue

```
        {
            "Effect": "Allow",
            "Action": [
                "glue:CreateDatabase",
                "glue:DeleteDatabase",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:UpdateDatabase",
                "glue:CreateTable",
                "glue:DeleteTable",
                "glue:GetTable",
                "glue:GetTables",
                "glue:UpdateTable"
            ],
```

```
            "Resource": [
                "arn:aws:glue:*:*:catalog",
                "arn:aws:glue:*:*:database/*",
                "arn:aws:glue:*:*:table/*/*",
                "arn:aws:glue:*:*:userDefinedFunction/*"
            ]
        }
```

- CloudWatch Autorisations relatives aux journaux

```
        {
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:PutLogEvents",
                "logs:DeleteLogGroup",
                "logs:DeleteLogStream",
                "logs:PutRetentionPolicy",
                "logs:DescribeLogGroups"
            ],
            "Resource": [
                "arn:aws:logs:*:*:log-group:/aws/lambda/*",
                "arn:aws:logs:*:*:log-group:*",
                "arn:aws:logs:*:*:log-group:/aws/kinesisfirehose/*"
            ]
        }
```

- CloudWatch Autorisations

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:DeleteDashboards",
                "cloudwatch:GetDashboard",
                "cloudwatch:ListDashboards",
                "cloudwatch:PutDashboard",
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*"
```

```
        }
```

- Autorisations SNS

```
        {
            "Effect": "Allow",
            "Action": [
                "sns:CreateTopic",
                "sns:DeleteTopic",
                "sns:Subscribe",
                "sns:Unsubscribe",
                "sns:SetTopicAttributes"
            ],
            "Resource": "arn:aws:sns:*:*:*"
        }
```

- Autorisations DynamoDB

```
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:CreateTable",
                "dynamodb:DeleteTable",
                "dynamodb:DescribeTable",
                "dynamodb:PutItem",
                "dynamodb:GetItem",
                "dynamodb:UpdateItem",
                "dynamodb:DeleteItem"
            ],
            "Resource": "arn:aws:dynamodb:*:*:table/*"
        }
```

- CloudFormation Autorisations

```
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
```

```
                "cloudformation:DescribeStacks",
                "cloudformation:UpdateStack",
                "cloudformation:ListStacks"
            ],
            "Resource": "arn:aws:cloudformation:*:*:stack/*/*"
        }
```

- Autorisations de registre de l'application Service Catalog

```
        {
            "Effect": "Allow",
            "Action": [
                "servicecatalog:CreateApplication",
                "servicecatalog:DeleteApplication",
                "servicecatalog:GetApplication",
                "servicecatalog:TagResource",
                "servicecatalog:CreateAttributeGroup",
                "servicecatalog:DeleteAttributeGroup",
                "servicecatalog:GetAttributeGroup",
                "servicecatalog:AssociateAttributeGroup",
                "servicecatalog:DisassociateAttributeGroup",
                "servicecatalog:AssociateResource",
                "servicecatalog:DisassociateResource"
            ],
            "Resource": "arn:aws:servicecatalog:*:*:*"
        }
```

- Autorisations X-Ray

```
        {
            "Effect": "Allow",
            "Action": [
                "xray:PutTraceSegments",
                "xray:PutTelemetryRecords"
            ],
            "Resource": "*"
        }
```

- Autorisations IAM

```
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:CreatePolicy",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DetachRolePolicy",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:ListRoles",
                "iam:PassRole",
                "iam:PutRolePolicy"
            ],
            "Resource": "arn:aws:iam::*:role/*"
        }
```

- EventBridge Autorisations

```
        {
            "Effect": "Allow",
            "Action": [
                "events:PutTargets",
                "events:RemoveTargets",
                "events:DescribeRule",
                "events:EnableRule",
                "events:ListRules",
                "events:PutRule",
                "events:DeleteRule",
                "events:ListEventSources",
                "events:DescribeEventSource",
                "events:ActivateEventSource",
                "events:DeactivateEventSource"
            ],
            "Resource": "arn:aws:events:*:*:rule/*"
        }
```

Déployez la solution

Cette solution utilise des CloudFormation modèles et des piles AWS pour automatiser son déploiement. Les CloudFormation modèles spécifient les ressources AWS incluses dans cette solution et leurs propriétés. La CloudFormation pile fournit les ressources décrites dans les modèles.

Vue d'ensemble du processus de déploiement

Avant de lancer le CloudFormation modèle, passez en revue les considérations relatives à l'architecture et à la configuration décrites dans ce guide. Suivez les step-by-step instructions de cette section pour configurer et déployer la solution dans votre compte.

Temps de déploiement : environ 15 minutes.

> **Note**
>
> Si vous avez déjà déployé cette solution, consultez Mettre à jour la solution pour obtenir des instructions de mise à jour.

Prérequis

- Configuration d'une CloudFront distribution
- Configuration d'un ALB

Étape 1. Lancez la pile

- Lancez le CloudFormation modèle sur votre compte AWS.
- Entrez des valeurs pour les paramètres requis : Stack Name et Application Access Log Bucket Name.
- Vérifiez les autres paramètres de modèle et ajustez-les si nécessaire.

Étape 2. Associez l'ACL Web à votre application Web

- Associez vos distributions CloudFront Web ou ALB à l'ACL Web générée par cette solution. Vous pouvez associer autant de distributions ou d'équilibreurs de charge que vous le souhaitez.

Étape 3. Configuration de la journalisation des accès Web

- Activez la journalisation des accès CloudFront Web pour vos distributions Web ou ALB, et envoyez les fichiers journaux au compartiment Amazon S3 approprié. Enregistrez les journaux dans un dossier correspondant au préfixe défini par l'utilisateur. Si aucun préfixe défini par l'utilisateur n'est utilisé, enregistrez les journaux dans AWSLogs (`AWSLogs/`préfixe de journal par défaut). Consultez le paramètre Application Access Log Bucket Prefix à l'étape 1. Lancez la pile pour plus d'informations.

CloudFormation Modèles AWS

Cette solution inclut un CloudFormation modèle AWS principal et deux modèles imbriqués. Vous pouvez télécharger les CloudFormation modèles avant de déployer la solution.

Pile principale

aws-waf-security-automations.template - Utilisez ce modèle comme point d'entrée pour lancer la solution dans votre compte. La configuration par défaut déploie une ACL Web AWS WAF avec des règles préconfigurées. Vous pouvez personnaliser le modèle en fonction de vos besoins.

pile WebACL

aws-waf-security-automations-webacl.template - Ce modèle imbriqué fournit des ressources AWS WAF, notamment une ACL Web, une adresse IP, des ensembles et d'autres ressources associées.

Pile Firehose Athena

aws-waf-security-automations-firehose-athena.template - Ce modèle imbriqué fournit des ressources liées à AWS Glue, Athena et Firehose. Il est créé lorsque vous choisissez l'analyseur de journaux Athena de Scanner & Probe ou l'analyseur de journaux HTTP Flood Lambda ou Athena.

> **Note**
>
> Les CloudFormation ressources AWS sont créées à partir des constructions du kit AWS Cloud Development Kit (AWS CDK).

Ce CloudFormation modèle AWS déploie la solution Security Automations for AWS WAF dans le cloud AWS.

Prérequis

Cette solution est conçue pour fonctionner avec des applications Web déployées avec CloudFront ou avec un ALB. Si aucune de ces ressources n'est déjà configurée, effectuez les tâches applicables avant de lancer cette solution.

Configuration d'une CloudFront distribution

Procédez comme suit pour configurer une CloudFront distribution pour le contenu statique et dynamique de votre application Web. Reportez-vous au manuel Amazon CloudFront Developer Guide pour obtenir des instructions détaillées.

1. Créez une distribution d'applications CloudFront Web. Reportez-vous à la section Création d'une distribution.
2. Configurez les origines statiques et dynamiques. Reportez-vous à la section Utilisation de différentes origines avec CloudFront les distributions.
3. Spécifiez le comportement de votre distribution. Reportez-vous aux valeurs que vous spécifiez lorsque vous créez ou mettez à jour une distribution.

> **Note**
>
> Si vous `CloudFront` le souhaitez comme point de terminaison, vous devez créer vos WAFV2 ressources dans la région USA Est (Virginie du Nord).

Configuration d'un ALB

Pour configurer un ALB afin de distribuer le trafic entrant vers votre application Web, reportez-vous à la section Créer un équilibreur de charge d'application dans le guide de l'utilisateur pour les équilibreurs de charge d'application.

Étape 1. Lancement de la pile

Ce CloudFormation modèle AWS automatisé déploie la solution sur le cloud AWS.

1. Connectez-vous à AWS Management Console et sélectionnez la solution de lancement pour lancer le `waf-automation-on-aws.template` CloudFormation modèle.

2. Le modèle est lancé par défaut dans la région USA Est (Virginie du Nord). Pour lancer cette solution dans une autre région AWS, utilisez le sélecteur de région dans la barre de navigation de la console. Si vous `CloudFront` le souhaitez comme point de terminaison, vous devez déployer la solution dans la région USA Est (Virginie du Nord`us-east-1`) ().

   > **Note**
   >
   > Selon les valeurs des paramètres d'entrée que vous définissez, cette solution nécessite différentes ressources. Ces ressources ne sont actuellement disponibles que dans certaines régions AWS. Par conséquent, vous devez lancer cette solution dans une région AWS où ces services sont disponibles. Pour plus d'informations, consultez la section Régions AWS prises en charge.

3. Sur la page Spécifier le modèle, vérifiez que vous avez sélectionné le bon modèle et choisissez Next.
4. Sur la page Spécifier les détails de la pile, attribuez un nom à votre configuration AWS WAF dans le champ Stack name. Il s'agit également du nom de l'ACL Web créée par le modèle.
5. Sous Paramètres, passez en revue les paramètres du modèle et modifiez-les si nécessaire. Pour désactiver une fonctionnalité particulière, sélectionnez none ou selon no le cas. Cette solution utilise les valeurs par défaut suivantes.

Paramètre	Par défaut	Description
Nom de la pile	`[.red]#<requires input>`	Le nom de la pile ne peut pas contenir d'espaces. Ce nom doit être unique dans votre compte AWS et il s'agit du nom de l'ACL Web créée par le modèle.
Type de ressource		
Point de terminaison	`CloudFront`	Choisissez le type de ressource utilisé. REMARQUE : Si vous le choisissez `CloudFront` comme point de terminaison, vous devez lancer la solution pour créer des ressource s WAF dans la région USA Est (Virginie du Nord) (`us-east-1`).
Groupes de règles de réputation IP gérés par AWS		

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés par la liste de réputation d'Amazon IP	no	Choisissez `yes` d'activer le composant conçu pour ajouter le groupe de règles géré par Amazon IP Reputation List à l'ACL Web. Ce groupe de règles est basé sur les informations internes d'Amazon sur les menaces. Cela 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. Le WCU requis est de 25. Votre compte doit disposer d'une capacité WCU suffisant e pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes de règles AWS Managed Rules.

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés par liste d'adresses IP anonymes	no	Choisissez `yes` d'activer le composant conçu pour ajouter un groupe de règles géré par liste d'adresses IP anonymes à l'ACL Web. Ce groupe de règles bloque les demandes provenant de services qui permetten t de masquer l'identité du spectateur. Il s'agit notamment des requêtes provenant de proxys VPNs, de nœuds Tor et de fournisse urs d'hébergement. 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 contribue r à limiter les robots et le non-respect des restrictions géographiques. Le WCU requis est de 50. Votre compte doit disposer d'une capacité WCU suffisant e pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité.

Paramètre	Par défaut	Description
		Pour plus d'informations, consultez la liste des groupes de règles AWS Managed Rules.
Groupes de règles de base gérés par AWS		

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés par un ensemble de règles de base	no	Choisissez `yes` d'activer le composant conçu pour ajouter le groupe de règles géré par un ensemble de règles de base à l'ACL Web. Ce groupe de règles fournit une protection contre l'exploitation d'un large éventail de vulnérabilités, y compris certaines des vulnérabilités les plus risquées et les plus courantes. Envisagez d'utiliser ce groupe de règles pour tous les cas d'utilisation d'AWS WAF. Le WCU requis est de 700. Votre compte doit disposer d'une capacité WCU suffisante pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes de règles AWS Managed Rules.

Paramètre	Par défaut	Description
Activer la protection des administrateurs, la protection des groupes de règles gérés	no	Choisissez `yes` d'activer le composant conçu pour ajouter le groupe de règles géré par Admin Protection à l'ACL Web. Ce groupe de règles bloque 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. Le WCU requis est de 100. Votre compte doit disposer d'une capacité WCU suffisante pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes de règles AWS Managed Rules.

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés contre les entrées défectueu ses connues	no	Choisissez `yes` d'activer le composant conçu pour ajouter le groupe de règles géré Known Bad Inputs à l'ACL Web. Ce groupe de règles bloque 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 malveilla nt accède à votre application comme administrateur. Le WCU requis est de 100. Votre compte doit disposer d'une capacité WCU suffisant e pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes de règles AWS Managed Rules.
Groupe de règles spécifiques aux cas d'utilisation gérés par AWS		

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés par la base de données SQL	no	Choisissez `yes` d'activer le composant conçu pour ajouter le groupe de règles géré par la base de données SQL à l'ACL Web. Ce groupe de règles bloque les modèles de demandes associés à l'exploitation de bases de données SQL, tels que les attaques par injection SQL. Cela peut aider à empêcher l'injecti on 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. L'utilisa tion de la règle personnalisée d'injection SQL est facultati ve si le groupe de règles SQL géré par AWS est déjà activé. Le WCU requis est de 200. Votre compte doit disposer d'une capacité WCU suffisant e pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes

Paramètre	Par défaut	Description
		de règles AWS Managed Rules.

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés par le système d'exploitation Linux	no	Choisissez `yes` d'activer le composant conçu pour ajouter le groupe de règles géré par le système d'exploitation Linux à l'ACL Web. Ce groupe de règles bloque les modèles de demandes associés à l'exploitation de vulnérabilités spécifiques à Linux, notamment les attaques d'inclusion de fichiers locaux (LFI) spécifiques 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. Évaluez 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 du système d'exploitation POSIX. Le WCU requis est de 200. Votre compte doit disposer d'une capacité WCU suffisante pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité.

Paramètre	Par défaut	Description
		Pour plus d'informations, consultez la liste des groupes de règles AWS Managed Rules.

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés par le système d'exploitation POSIX	no	Choisissez `yes` d'activer le composant conçu pour ajouter la protection des groupes de règles gérés par un ensemble de règles de base à l'ACL Web. Ce groupe de règles bloque les modèles de demandes associés à l'exploitation de vulnérabilités spécifiques aux systèmes d'exploitation POSIX et de type POSIX, y compris les attaques LFI. 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. Évaluez ce groupe de règles si une partie de votre application s'exécute sur un système d'exploitation POSIX ou de type POSIX. Le WCU requis est de 100. Votre compte doit disposer d'une capacité WCU suffisant e pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes

Paramètre	Par défaut	Description
		de règles AWS Managed Rules.

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés par le système d'exploitation Windows	no	Choisissez `yes` d'activer le composant conçu pour ajouter le groupe de règles géré par le système d'exploitation Windows à l'ACL Web. Ce groupe de règles bloque 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. Le WCU requis est de 200. Votre compte doit disposer d'une capacité WCU suffisante pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes

Paramètre	Par défaut	Description
		de règles AWS Managed Rules.

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés par les applications PHP	no	Choisissez `yes` d'activer le composant conçu pour ajouter le groupe de règles géré par l'application PHP à l'ACL Web. Ce groupe de règles bloque les modèles de demandes associés à l'exploitation de vulnérabilités spécifiques à l'utilisation du langage de programmation PHP, notamment l'injection de fonctions PHP non sécurisée s. 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. Le WCU requis est de 100. Votre compte doit disposer d'une capacité WCU suffisant e pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes

Paramètre	Par défaut	Description
		de règles AWS Managed Rules.
Activer la protection des groupes de règles gérée par les WordPress applications	no	Choisissez `yes` d'activer le composant conçu pour ajouter le groupe de règles géré par l'WordPress application à l'ACL Web. Ce groupe de règles bloque les modèles de demandes associés à l'exploitation de vulnérabilités spécifiques aux WordPress sites. Évaluez ce groupe de règles si vous courez WordPress. Ce groupe de règles doit être utilisé conjointement avec la base de données SQL et les groupes de règles d'application PHP. Le WCU requis est de 100. Votre compte doit disposer d'une capacité WCU suffisante pour éviter l'échec du déploiement de la pile ACL Web en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes de règles AWS Managed Rules.

Paramètre	Par défaut	Description
Règle personnalisée - Scanner et sondes		
Activer la protection du scanner et de la sonde	`yes - AWS Lambda log parser`	Choisissez le composant utilisé pour bloquer les scanners et les sondes. Reportez-vous à la section Options de l'analyseur Log pour plus d'informations sur les compromis liés aux options d'atténuation.

Paramètre	Par défaut	Description
Nom du compartiment du journal d'accès aux applications	`[.red]<requires input>`	Si vous avez choisi `yes` le paramètre Activate Scanner & Probe Protection, entrez le nom du compartiment Amazon S3 (nouveau ou existant) dans lequel vous souhaitez stocker les journaux d'accès pour vos CloudFront distributions ou ALB. Si vous utilisez un compartiment Amazon S3 existant, celui-ci doit être situé dans la même région AWS où vous déployez le CloudFormation modèle. Vous devez utiliser un compartiment différent pour chaque déploiement de solution. Pour désactiver cette protection, ignorez ce paramètre. REMARQUE : Activez la journalisation des accès CloudFront Web pour vos distributions Web ou ALB afin d'envoyer des fichiers journaux à ce compartiment Amazon S3. Enregistrez les journaux dans le même préfixe défini dans la pile (préfixe `AWSLogs/` par défaut). Consultez le paramètre Application Access

Paramètre	Par défaut	Description
		Log Bucket Prefix pour plus d'informations.
Préfixe du compartiment du journal d'accès aux applications	`AWSLogs/`	Si vous avez choisi `yes` le paramètre Activate Scanner & Probe Protection, vous pouvez entrer un préfixe facultatif défini par l'utilisateur pour le bucket de journaux d'accès aux applications ci-dessus. Si vous avez choisi `CloudFront` le paramètre Endpoint, vous pouvez saisir n'importe quel préfixe tel que`yourprefix/` . Si vous avez choisi `ALB` le paramètre Endpoint, vous devez l'ajouter `AWSLogs/` à votre préfixe tel que. `yourprefix/AWSLogs/` Utiliser `AWSLogs/` (par défaut) s'il n'existe pas de préfixe défini par l'utilisateur. Pour désactiver cette protection, ignorez ce paramètre.

Paramètre	Par défaut	Description
La journalisation des accès aux compartiments est-elle activée ?	no	Choisissez yes si vous avez saisi un nom de compartiment Amazon S3 existant pour le paramètre Application Access Log Bucket Name et si la journalisation des accès au serveur pour le compartiment est déjà activée. Si vous le souhaitezno, la solution active la journalisation des accès au serveur pour votre bucket. Si vous avez choisi no le paramètre Activate Scanner & Probe Protection, ignorez-le.
Seuil d'erreur	50	Si vous avez choisi yes le paramètre Activate Scanner & Probe Protection, entrez le nombre maximum de mauvaises demandes acceptables par minute et par adresse IP. Si vous avez choisi no le paramètre Activate Scanner & Probe Protection, ignorez-le.

Paramètre	Par défaut	Description
Conservez les données dans leur emplacement S3 d'origine	no	Si vous avez choisi `yes - Amazon Athena log parser` le paramètre Activate Scanner & Probe Protection, la solution applique le partitionnement aux fichiers journaux d'accès aux applications et aux requêtes Athena. Par défaut, la solution déplace les fichiers journaux de leur emplacement d'origine vers une structure de dossiers partitionnée dans Amazon S3. Choisissez `yes` si vous souhaitez également conserver une copie des journaux dans leur emplacement d'origine. Cela dupliquera le stockage de vos journaux. Si vous n'avez pas choisi `yes - Amazon Athena log parser` le paramètre Activer la protection du scanner et de la sonde, ignorez-le.
Règle personnalisée - HTTP Flood		

Paramètre	Par défaut	Description
Activer la protection HTTP contre les inondations	`yes - AWS WAF rate-based rule`	Sélectionnez le composant utilisé pour bloquer les attaques HTTP flood. Reportez-vous à la section Options de l'analyseur Log pour plus d'informations sur les compromis liés aux options d'atténuation.
Seuil de demande par défaut	`100`	Si vous avez choisi `yes` le paramètre Activer la protection HTTP Flood, entrez le nombre maximal de demandes acceptables toutes les cinq minutes, par adresse IP. Si vous avez choisi `yes - AWS WAF rate-based rule` le paramètre Activer la protection HTTP contre les inondations, la valeur minimale acceptable est`10`. Si vous avez choisi `yes - AWS Lambda log parser` ou `yes - Amazon Athena log parser` pour le paramètre Activate HTTP Flood Protection, il peut s'agir de n'importe quelle valeur. Pour désactiver cette protection, ignorez ce paramètre.

Paramètre	Par défaut	Description
Seuil de demande par pays	<optional input>	Si vous avez choisi `yes - Amazon Athena log parser` le paramètre Activer la protection HTTP contre les inondations, vous pouvez entrer un seuil par pays en suivant ce format JSON`{"TR":50, "ER":150}` . La solution utilise ces seuils pour les demandes provenant des pays spécifiés. La solution utilise le paramètre Default Request Threshold pour les demandes restantes . REMARQUE : Si vous définissez ce paramètre , le pays sera automatiq uement inclus dans le groupe de requêtes Athena, ainsi que l'adresse IP et les autres champs facultatifs de regroupement que vous pouvez sélectionner avec le paramètre de requête Group By Requests in HTTP Flood Athena Query. + Si vous avez choisi de désactiver cette protection, ignorez ce paramètre.

Paramètre	Par défaut	Description
Regrouper par requêtes dans HTTP Flood Athena Query	`None`	Si vous avez choisi `yes - Amazon Athena log parser` le paramètre Activer la protection HTTP contre les inondations, vous pouvez choisir un champ groupé pour compter les demandes par adresse IP et le champ groupé sélectionné. Par exemple, si vous le souhaitez `URI`, la solution compte les demandes par IP et par URI. Si vous avez choisi de désactiver cette protection, ignorez ce paramètre.
Période de blocage du WAF	`240`	Si vous avez choisi `yes - AWS Lambda log parser` `yes - Amazon Athena log parser` les paramètres Activate Scanner & Probe Protection ou Activate HTTP Flood Protection, entrez la période (en minutes) pour bloquer les adresses IP applicables. Pour désactiver l'analyse des journaux, ignorez ce paramètre.

Paramètre	Par défaut	Description
Calendrier d'exécution des requêtes Athena (minutes)	5	Si vous avez choisi `yes - Amazon Athena log parser` les paramètres Activate Scanner & Probe Protection ou Activate HTTP Flood Protection, vous pouvez saisir un intervalle de temps (en minutes) pendant lequel la requête Athena s'exécute. Par défaut, la requête Athena est exécutée toutes les 5 minutes. Si vous avez choisi de désactiver ces protections, ignorez ce paramètre.

Paramètre	Par défaut	Description
Clés de règles	`IP`	Si vous avez choisi `yes - AWS WAF rate-based rule` le paramètre Activate HTTP Flood Protection, configurez cette règle pour utiliser diverses autres combinaisons de clés d'agrégation. Options disponibles : IP (par défaut) IP+en-tête personnalisé (si cette option est sélectionnée, `Rule Keys Custom Header` elle est obligatoire) IP+URI MÉTHODE IP+HTTP Pour plus d'informations, consultez la section Options d'agrégation basées sur le taux des règles WAF.

Paramètre	Par défaut	Description
En-tête personnalisé de Rule Keys	no	Si vous avez choisi `IP +Custom Header` le paramètre Rule Keys, entrez le nom de l'en-tête personnalisé à utiliser pour l'agrégation des demandes. Pour plus d'informations, voir Options d'agrégation basées sur le taux de type d'instruction de règle WAF.

Paramètre	Par défaut	Description
Seuil de fenêtre temporelle (minutes)	5	Seuil temporel en minutes pour la protection HTTP contre les inondations. S'applique à la fois à la règle basée sur le taux et à l'analyseur de log Lambda. Options disponibles : [1, 2, 5, 10]. Si vous avez choisi `yes - AWS WAF rate-based rule` le paramètre Activate HTTP Flood Protection, il sera utilisé pour les fenêtres temporelles d'évaluation. Pour plus d'informations, consultez la déclaration basée sur le taux d'ACL Web du WAF. Si vous avez choisi `yes - AWS Lambda log parser` le paramètre Activate HTTP Flood Protection, il sera utilisé pour la période d'évaluation en plus de la période de blocage.
Règle personnalisée - Bad Bot		

Paramètre	Par défaut	Description
Activer la protection contre les robots malveillants	`yes`	Choisissez `yes` d'activer le composant conçu pour bloquer les robots malveillants et les scrapeurs de contenu.
ARN d'un rôle IAM disposant d'un accès en écriture aux CloudWatch journaux de votre compte	<optional input>	Fournissez un ARN facultatif pour un rôle IAM disposant d'un accès en écriture aux CloudWatch journaux de votre compte. Par exemple : `ARN: arn:aws:iam::account_id:role/myrolename` . Si vous laissez ce paramètre vide (par défaut), la solution vous crée un nouveau rôle.
Règle personnalisée - Listes de réputation IP de tiers		
Activer la protection des listes de réputation	`yes`	Choisissez de `yes` bloquer les demandes provenant d'adresses IP figurant sur des listes de réputation tierces (les listes prises en charge incluent Spamhaus, Emerging Threats et le nœud de sortie Tor).
Règles personnalisées héritées		

Paramètre	Par défaut	Description
Activer la protection contre les injections SQL	`yes`	Choisissez `yes` d'activer le composant conçu pour bloquer les attaques par injection SQL courantes. Envisagez de l'activer si vous n'utilisez pas un ensemble de règles principales géré par AWS ou un groupe de règles de base de données SQL géré par AWS. Vous pouvez choisir l'une des options `yes` (continue r) ou`yes - NO_MATCH`) selon laquelle vous souhaitez qu'AWS WAF gère les demandes surdimensionnées supérieures à 8 Ko (8192 octets). `yes - MATCH` Par défaut, `yes` inspecte le contenu du composant de demande qui respecte les limites de taille conformém ent aux critères d'inspect ion des règles. Pour plus d'informations, reportez-vous à la section Gestion des composants de requêtes Web surdimensionnés. Choisissez no de désactive r cette fonctionnalité. REMARQUE : La CloudForm ation pile ajoute l'option de gestion des surdimens

Paramètre	Par défaut	Description
		ionnements sélectionnée à la règle de protection par injection SQL par défaut et la déploie dans votre compte AWS. Si vous avez personnalisé la règle en dehors de CloudFormation, vos modifications seront remplacées après la mise à jour de la pile.

Paramètre	Par défaut	Description
Niveau de sensibilité pour la protection contre les injections SQL	`LOW`	Choisissez le niveau de sensibilité que vous souhaitez qu'AWS WAF utilise pour détecter les attaques par injection de code SQL. `HIGH`détecte davantage d'attaques, mais peut générer davantage de faux positifs. `LOW` est généralement un meilleur choix pour les ressources qui disposent déjà d'autres protections contre les attaques par injection SQL ou qui ont une faible tolérance aux faux positifs. Pour plus d'informations, reportez-vous à AWS WAF qui ajoute des niveaux de sensibilité pour les instructions de règles d'injection SQL et les SensitivityLevel propriétés dans le guide de CloudFormation l'utilisateur AWS. Si vous choisissez de désactiver la protection contre les injections SQL, ignorez ce paramètre. REMARQUE : La CloudFormation pile ajoute le niveau de sensibilité sélectionné à la règle de protection par

Paramètre	Par défaut	Description
		injection SQL par défaut et le déploie dans votre compte AWS. Si vous avez personnalisé la règle en dehors de CloudFormation, vos modifications seront remplacées après la mise à jour de la pile.

Paramètre	Par défaut	Description
Activer la protection contre les scripts intersites	`yes`	Choisissez `yes` d'activer le composant conçu pour bloquer les attaques XSS courantes. Envisagez de l'activer si vous n'utilisez pas un ensemble de règles de base géré par AWS. Vous pouvez également sélectionner l'une des options (`yes`(continuer) ou`yes - NO_MATCH`) selon laquelle vous souhaitez qu'AWS WAF gère les demandes surdimensionnées supérieur es à 8 Ko (8192 octets). `yes - MATCH` Par défaut, `yes` utilise l'`Continue`option, qui inspecte le contenu du composant de demande qui respecte les limites de taille conformément aux critères d'inspection des règles. Pour plus d'informations, reportez-vous à la section Gestion des composants de demande surdimensionnés. Choisissez no de désactive r cette fonctionnalité. REMARQUE : La CloudForm ation pile ajoute l'option de gestion des surdimens ionnements sélectionnée à la règle de script intersite par défaut et la déploie dans

Paramètre	Par défaut	Description
		votre compte AWS. Si vous avez personnalisé la règle en dehors de CloudFormation, vos modifications seront remplacées après la mise à jour de la pile.
Paramètres de conservation des adresses IP autorisés et refusés		
Période de rétention (minutes) pour l'ensemble d'adresses IP autorisé	`-1`	Si vous souhaitez activer la conservation des adresses IP pour l'ensemble d'adresses IP autorisées, entrez un nombre (`15`ou plus) comme période de rétention (minutes). Les adresses IP qui atteignent la période de conservation expirent et la solution les supprime de l'ensemble d'adresses IP. La solution prend en charge une période de conservation minimale de 15 minutes. Si vous entrez un nombre compris entre `0` et`15`, la solution le traite comme`15`. Laissez-le tel quel `-1` (par défaut) pour désactiver la conservation des adresses IP.

Paramètre	Par défaut	Description
Période de rétention (minutes) pour l'ensemble d'adresses IP refusées	`-1`	Si vous souhaitez activer la rétention IP pour l'ensembl e d'adresses IP refusées, entrez un nombre (`15`ou plus) comme période de rétention (minutes). Les adresses IP qui atteignent la période de conservation expirent et la solution les supprime de l'ensemble d'adresses IP. La solution prend en charge une période de conservat ion minimale de 15 minutes. Si vous entrez un nombre compris entre `0` et`15`, la solution le traite comme`15`. Laissez-le tel quel `-1` (par défaut) pour désactiver la conservation des adresses IP.

Paramètre	Par défaut	Description
E-mail pour recevoir une notification en cas d'expiration des ensembles d'adresses IP autorisés ou refusés	<optional input>	Si vous avez activé les paramètres de période de conservation des adresses IP (voir les deux paramètres précédents) et que vous souhaitez recevoir une notification par e-mail lorsque les adresses IP expirent, entrez une adresse e-mail valide. Si vous n'avez pas activé la conservation de l'adresse IP ou si vous souhaitez désactiver les notifications par e-mail, laissez ce champ vide (par défaut).
Réglages avancés		
Période de conservation (jours) pour les groupes de journaux	365	Si vous souhaitez activer la conservation pour les groupes de CloudWatch journaux, entrez un nombre (1ou plus) comme période de conservation (jours). Vous pouvez choisir une durée de conservation comprise entre un jour (1) et dix ans (3650). Par défaut, les journaux expirent au bout d'un an. Réglez-le sur -1 pour conserver les journaux indéfiniment.

6. Choisissez Suivant.
7. Sur la page Configurer les options de pile, vous pouvez spécifier des balises (paires clé-valeur) pour les ressources de votre pile et définir des options supplémentaires. Choisissez Suivant.
8. Sur la page Réviser et créer, vérifiez et confirmez les paramètres. Cochez les cases indiquant que le modèle créera des ressources IAM et toutes les fonctionnalités supplémentaires requises.
9. Choisissez Submit pour déployer la pile.

   Consultez l'état de la pile dans la CloudFormation console AWS dans la colonne Status. Vous devriez recevoir le statut CREATE_COMPLETE dans 15 minutes environ.

> **Note**
>
> Outre les fonctions `Log Parser` et `IP Lists Parser` AWS Lambda, cette solution inclut les fonctions et `helper` `custom-resource` Lambda, qui s'exécutent uniquement lors de la configuration initiale ou lorsque les ressources sont mises à jour ou supprimées. Lorsque vous utilisez cette solution, toutes les fonctions s'affichent dans la console AWS Lambda, mais seules les trois fonctions principales de la solution sont régulièrement actives. Ne supprimez pas les deux autres fonctions ; elles sont nécessaires pour gérer les ressources associées.

Pour obtenir des informations détaillées sur les ressources de la pile, cliquez sur l'onglet Sorties. Cela inclut la BadBotHoneypotEndpointvaleur. N'oubliez pas cette valeur car elle sera utilisée dans Intégrer le lien Honeypot dans votre application Web.

Étape 2. Associez l'ACL Web à votre application Web

Mettez à jour vos CloudFront distributions ou ALB pour activer AWS WAF et la journalisation à l'aide des ressources que vous avez générées à l'étape 1. Lancez la pile.

1. Connectez-vous à la console AWS WAF.
2. Choisissez l'ACL Web que vous souhaitez utiliser.
3. Sous l'onglet Ressources AWS associées, choisissez Ajouter des ressources AWS.
4. Sous Type de ressource, choisissez la CloudFront distribution ou ALB.
5. Sélectionnez une ressource dans la liste, puis choisissez Ajouter pour enregistrer vos modifications.

Étape 3. Configuration de la journalisation des accès web

CloudFront Configurez votre ALB pour envoyer les journaux d'accès Web au compartiment Amazon S3 approprié afin que ces données soient disponibles pour la fonction Lambda du Log Parser.

Stocker les journaux d'accès Web d'une CloudFront distribution

1. Connectez-vous à la CloudFront console Amazon.
2. Sélectionnez la distribution de votre application Web, puis sélectionnez Paramètres de distribution.
3. Sous l'onglet General, choisissez Edit.
4. Pour AWS WAF Web ACL, choisissez la solution ACL Web créée (le paramètre Stack name).
5. Pour Journalisation, choisissez Activé.
6. Pour Bucket for Logs, choisissez le compartiment S3 que vous souhaitez utiliser pour stocker les journaux d'accès au Web. Il peut s'agir d'un compartiment S3 nouveau ou existant utilisé dans la pile principale et autorisé CloudFront à écrire des journaux. La liste déroulante répertorie les buckets associés au compte AWS actuel. Pour plus d'informations, consultez Getting started with a basic CloudFront distribution dans le manuel Amazon CloudFront Developer Guide.
7. Définissez le préfixe du journal sur le préfixe utilisé pour déployer la solution. Vous pouvez trouver le préfixe dans la pile principale, onglet Paramètres AppAccessLogBucketPrefixParam(par défaut`AWSLogs/`).
8. Pour enregistrer vos modifications, choisissez Oui, modifier.

Pour plus d'informations, reportez-vous à la section Configuration et utilisation de journaux standard (journaux d'accès) dans le manuel Amazon CloudFront Developer Guide.

Stocker les journaux d'accès au Web à partir d'un Application Load Balancer

1. Connectez-vous à la console Amazon Elastic Compute Cloud (Amazon EC2).
2. Dans le volet de navigation, choisissez Load Balancers.
3. Sélectionnez l'ALB de votre application Web.
4. Dans l'onglet Description, choisissez Modifier des attributs.
5. Choisissez Activer les journaux d'accès.

6. Pour l'emplacement S3, tapez le nom du compartiment S3 que vous souhaitez utiliser pour stocker les journaux d'accès Web. Il peut s'agir d'un compartiment S3 nouveau ou existant utilisé dans la pile principale et autorisé Application Load Balancer à écrire des journaux.
7. Définissez le préfixe du journal sur le préfixe utilisé pour déployer la solution. Vous pouvez trouver le préfixe dans la pile principale, onglet Paramètres AppAccessLogBucketPrefixParam(par défaut`AWSLogs/`).
8. Choisissez Enregistrer.

Pour plus d'informations, reportez-vous aux journaux d'accès de votre Application Load Balancer dans le guide de l'utilisateur d'Elastic Load Balancing.

Mettre à jour la solution

Si vous avez déjà déployé la solution, suivez cette procédure pour mettre à jour la CloudFormation pile de la solution afin d'obtenir la dernière version du framework de la solution. Avant de mettre à jour la pile, lisez attentivement les considérations relatives à la mise à jour.

1. Connectez-vous à la CloudFormation console AWS.
2. Sélectionnez Stacks dans le menu de navigation de gauche.
3. Sélectionnez votre `aws-waf-security-automations` CloudFormation stack existant.
4. Choisissez Mettre à jour.
5. Sélectionnez Remplacer le modèle actuel.
6. Sous Spécifier le modèle :
   a. Sélectionnez l'URL Amazon S3.
   b. Copiez le lien de l'`aws-waf-security-automations.template`AWS CloudFormation.
   c. Collez le lien dans le champ URL d'Amazon S3.
   d. Vérifiez que l'URL du modèle s'affiche correctement dans la zone de texte URL Amazon S3.
   e. Choisissez Suivant.
   f. Choisissez Suivant à nouveau.
7. Sous Paramètres, passez en revue les paramètres du modèle et modifiez-les si nécessaire. Reportez-vous à l'étape 1. Lancez la pile pour plus de détails sur les paramètres.
8. Choisissez Next (Suivant).
9. Sur la page Configurer les options de pile, choisissez Suivant.
10. Sur la page Vérification, vérifiez et confirmez les paramètres.
11. Cochez la case indiquant que le modèle est susceptible de créer des ressources IAM.
12. Choisissez Afficher l'ensemble de modifications et vérifiez les modifications.
13. Choisissez Mettre à jour la pile pour déployer la pile.

Vous pouvez voir l'état de la pile dans la CloudFormation console AWS dans la colonne Status. Vous devriez voir le statut UPDATE_COMPLETE dans 15 minutes environ.

Considérations relatives aux mises

Les sections suivantes présentent les contraintes et les considérations relatives à la mise à jour de cette solution.

Mise à jour du type de ressource

Vous devez déployer une nouvelle pile pour mettre à jour le paramètre Endpoint après avoir créé la pile. Ne modifiez pas le paramètre Endpoint lors de la mise à jour de la pile.

WAFV2 mise à niveau

À partir de la version 3.0, cette solution prend en charge AWS WAFV2. Nous avons remplacé tous les appels d'API AWS WAF Classic par des appels d'API WAFV2 AWS. Cela supprime les dépendances vis-à-vis de Node.js et utilise le plus d'environnement d'exécution up-to-date Python. Pour continuer à utiliser cette solution avec les dernières fonctionnalités et améliorations, vous devez déployer la version 3.0 ou supérieure en tant que nouvelle pile.

Personnalisations lors de la mise à jour de Stack

La out-of-box solution déploie un ensemble de règles AWS WAF avec des configurations par défaut dans votre compte AWS avec CloudFormation la pile. Nous ne recommandons pas d'appliquer des personnalisations aux règles déployées par la solution. Les mises à jour de Stack remplacent ces modifications. Si vous avez besoin de règles personnalisées, nous vous recommandons de créer des règles distinctes en dehors de la solution.

Mise à niveau de Bad Bot Protection

Dans la version 4.1.0, le gestionnaire d'accès Lambda avec API Gateway est devenu obsolète et remplacé par une fonctionnalité de journalisation améliorée issue de cette fonctionnalité. `Log parser - Bad bot` Au lieu d'utiliser des requêtes directes via API Gateway, la solution réutilise désormais le flux de log pour détecter les bots malveillants.

Mise en œuvre précédente :

1. Gestionnaire d'accès Lambda et API Gateway requis.
2. Point de terminaison Honeypot utilisé pour le traitement direct des demandes.
3. Nécessité d'intégrer le point de terminaison Honeypot dans les sites Web.

Nouvelle implémentation (version 4.1.0+) : l'analyseur de journaux Bad Bot Protection est désormais disponible :

1. Inspecte les demandes adressées au point de terminaison Honeypot via des journaux.
2. Traite les demandes lorsque la protection contre les robots malveillants est activée.
3. Utilise le filtre WAF BadBotRuleFilterpour identifier les mauvaises demandes de bot.
4. Analyse les données du journal pour identifier les adresses IP dépassant les quotas définis.
5. Met à jour les conditions définies par AWS WAF IP pour bloquer les adresses identifiées.

Cette modification simplifie l'architecture en éliminant les fonctionnalités dupliquées et en tirant parti des capacités de traitement des journaux existantes.

Mise à niveau du CDK

À partir de la version v4.1.0, cette solution est prise en charge par CDK. Si vous migrez depuis une version inférieure à la version 4.1.0. Utilisez le nouveau modèle et la nouvelle solution de mise à jour dans Cloudformation. Vous pouvez ensuite commencer à mettre à jour la solution localement via votre terminal à l'aide de cdk deploy (voir README pour plus d'informations). Si vous essayez d'utiliser directement cdk deploy, vous pouvez voir cette erreur : indentation insuffisante dans la collecte de flux

L'autre moyen de mettre à jour la solution consiste à utiliser le modèle fourni par la solution et à accéder à la section Cloudformation de la console AWS, à cliquer sur mettre à jour la solution et à y coller le nouveau modèle.

> **Note**
>
> Si vous effectuez une mise à niveau de la version 3.0 ou 3.1 vers la version 3.2 ou une version ultérieure de cette solution et que vous avez inséré manuellement des adresses IP dans l'ensemble d'adresses IP autorisées ou refusées, vous risquez de perdre ces adresses IP. Pour éviter que cela ne se produise, faites une copie des adresses IP incluses dans l'ensemble d'adresses IP autorisées ou refusées avant de mettre à niveau la solution. Ensuite, une fois la mise à niveau terminée, ajoutez à nouveau les adresses IP à l'ensemble d'adresses IP selon les besoins. Reportez-vous aux commandes get-ip-setet update-ip-setCLI. Si vous utilisez déjà la version 3.2 ou une version plus récente, ignorez cette étape.

Désinstallez la solution

Pour désinstaller la solution, supprimez les CloudFormation piles :

1. Connectez-vous à la CloudFormation console AWS.
2. Sélectionnez la pile parent de la solution. Toutes les autres piles de solutions seront automatiquement supprimées.
3. Sélectionnez Delete (Supprimer).

> **Note**
>
> La désinstallation de la solution supprime toutes les ressources AWS utilisées par la solution, à l'exception des compartiments Amazon S3. Si certains ensembles d'adresses IP ne sont pas supprimés en raison d'un problème de dépassement du débit dû aux quotas de l'API AWA WAF, supprimez manuellement ces ensembles d'adresses IP, puis supprimez la pile.

Utilisez la solution

Cette section fournit des instructions détaillées pour utiliser la solution une fois que vous l'avez déployée.

Modifier les ensembles d'adresses IP autorisés et refusés (facultatif)

Après avoir déployé la CloudFormation pile de cette solution, vous pouvez modifier manuellement les ensembles d'adresses IP autorisés et refusés pour ajouter ou supprimer des adresses IP selon les besoins.

1. Connectez-vous à la console AWS WAF.
2. Dans le volet de navigation de gauche, sélectionnez IP Sets.
3. Choisissez l'adresse IP définie pour la liste autorisée et ajoutez des adresses IP provenant de sources fiables.
4. Choisissez l'adresse IP définie pour la liste des adresses refusées et ajoutez les adresses IP que vous souhaitez bloquer.

Intégrez le lien Honeypot dans votre application Web (facultatif)

Si vous avez choisi `yes` le paramètre Activate Bad Bot Protection à l'étape 1. Lancez la pile, le CloudFormation modèle crée un point de terminaison piège vers un pot de production à faible interaction. Ce piège est destiné à détecter et à détourner les demandes entrantes provenant des scrapeurs de contenu et des robots malveillants. Les utilisateurs valides ne tenteront pas d'accéder à ce point de terminaison.

Ce composant améliore la détection des robots malveillants en surveillant les connexions directes à un Application Load Balancer (ALB) ou à Amazon CloudFront, en plus du mécanisme Honeypot. Si un bot contourne le honeypot et tente d'interagir avec ALB CloudFront, le système analyse les modèles de demandes et les journaux pour identifier les activités malveillantes. Lorsqu'un robot malveillant est détecté, son adresse IP est extraite et ajoutée à une liste de blocage AWS WAF pour empêcher tout accès ultérieur. La détection des bots défectueux s'effectue par le biais d'une chaîne logique structurée, garantissant une couverture complète des menaces :

- Analyseur de journal Lambda HTTP Flood Protection : collecte les bots défectueux à IPs partir des entrées du journal lors de l'analyse des inondations.
- Analyseur de journal Lambda pour la protection des scanners et des sondes : identifie les robots défectueux à IPs partir des entrées du journal relatives au scanner.
- Analyseur de journaux Athena pour la protection contre les inondations HTTP : extrait les robots malveillants des journaux IPs Athena, en utilisant des partitions lors de l'exécution des requêtes.
- Scanner & Probe Protection Athena Log Parser : récupère les robots malveillants des journaux Athena IPs liés au scanner, en utilisant la même stratégie de partitionnement.
- Détection des failles : si la protection HTTP contre les inondations et la protection contre les scanners et les sondes sont désactivées, le système s'appuie sur l'analyseur Log Lambda, qui enregistre l'activité des robots en fonction des filtres d'étiquettes WAF.

Utilisez l'une des procédures suivantes pour intégrer le lien Honeypot pour les demandes provenant de l'une CloudFront ou l'autre distribution.

Création d'une CloudFront origine pour le point de terminaison Honeypot

Utilisez cette procédure pour les applications Web déployées avec une CloudFront distribution. Avec CloudFront, vous pouvez inclure un `robots.txt` fichier pour aider à identifier les scrapeurs de contenu et les robots qui ignorent la norme d'exclusion des robots. Procédez comme suit pour intégrer le lien masqué, puis l'interdire explicitement dans votre `robots.txt` fichier.

1. Connectez-vous à la CloudFormation console AWS.
2. Choisissez la pile que vous avez construite à l'étape 1. Lancez la pile
3. Choisissez l'onglet Outputs.
4. À partir de la BadBotHoneypotEndpointclé, copiez l'URL du point de terminaison.
   - Le chemin du comportement (`/ProdStage`)
5. Intégrez ce lien de point de terminaison dans votre contenu pointant vers le honeypot. Cachez ce lien à vos utilisateurs humains. À titre d'exemple, consultez l'exemple de code suivant : `<a href="/behavior_path" rel="nofollow" style="display: none" aria-hidden="true">honeypot link</a>`
6. Modifiez le `robots.txt` fichier situé à la racine de votre site Web pour interdire explicitement le lien Honeypot, comme suit :

```
User-agent: <*>
        Disallow: /<behavior_path>
```

Important

Aucun enregistrement de chemin n' CloudFront est requis car les demandes sont : bloquées par le WAF BadBotRuleFilter. Solution collectée automatiquement dans les journaux. Traité par l'analyseur Log Lambda. Cette approche simplifiée utilise directement les journaux WAF au lieu de nécessiter une configuration de point de terminaison supplémentaire, ce qui rend le processus de détection des robots défectueux plus efficace grâce à l'analyse des journaux

Note

Il est de votre responsabilité de vérifier quelles valeurs de balise fonctionnent dans l'environnement de votre site Web. Ne l'utilisez pas `rel="nofollow"` si votre environnement ne le respecte pas. Pour plus d'informations sur la configuration des balises méta des robots, consultez le guide du développeur de Google. Modifiez le `robots.txt` fichier situé à la racine de votre site Web pour interdire explicitement le lien Honeypot, comme suit :

Intégrer le point de terminaison Honeypot en tant que lien externe

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.

Utilisez cette procédure pour les applications Web.

1. Connectez-vous à la CloudFormation console AWS.
2. Choisissez la pile que vous avez construite à l'étape 1. Lancez la pile.
3. Choisissez l'onglet Outputs.

4. À partir de la BadBotHoneypotEndpointclé, copiez l'URL du point de terminaison.

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

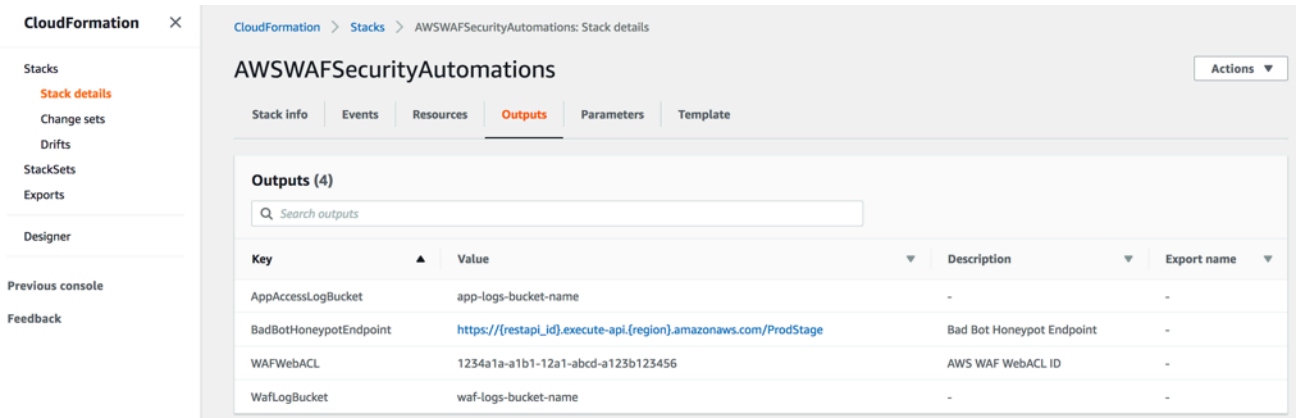
> **Note**
>
> Cette procédure permet d'indiquer `rel=nofollow` aux robots de ne pas accéder à l'URL du honeypot. Toutefois, étant donné que le lien est intégré en externe, vous ne pouvez pas inclure de `robots.txt` fichier interdisant explicitement le lien. Il est de votre responsabilité de vérifier quelles balises fonctionnent dans l'environnement de votre site Web. Ne l'utilisez pas `rel="nofollow"` si votre environnement ne le respecte pas.

Utiliser le fichier JSON de l'analyseur de journal Lambda

Utiliser le fichier JSON de l'analyseur de journal Lambda pour la protection HTTP Flood

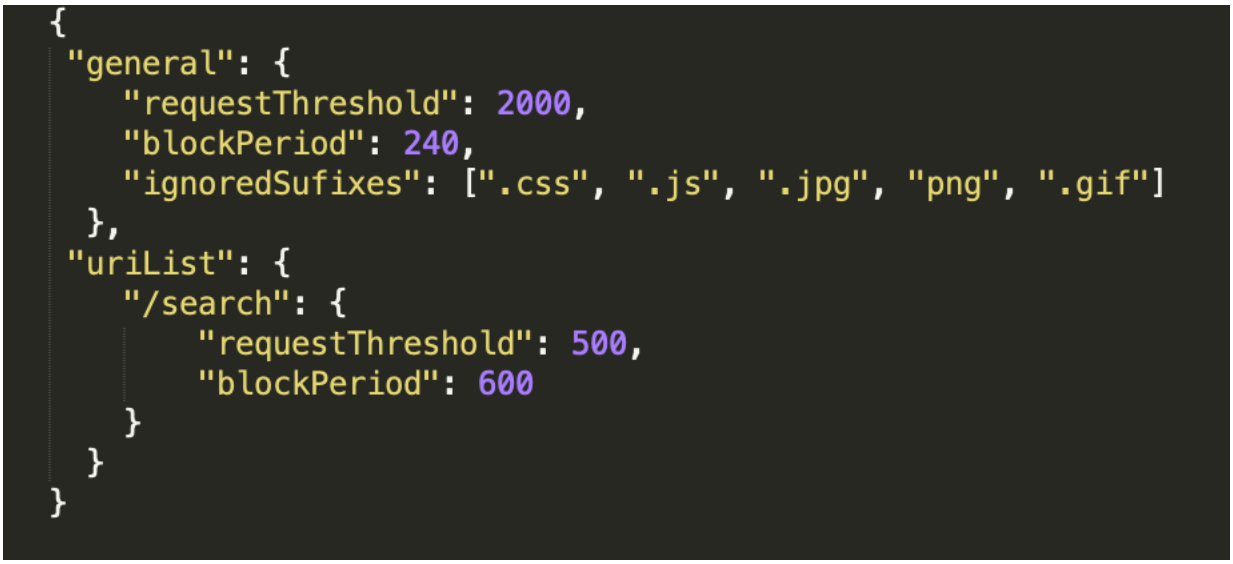
Si vous avez choisi `Yes - AWS Lambda log parser` le paramètre de modèle Activate HTTP Flood Protection, cette solution crée un fichier de configuration nommé `<stack_name>-waf_log_conf.json` et le télécharge dans le compartiment Amazon S3 utilisé pour stocker les fichiers journaux AWS WAF. Pour trouver le nom du compartiment, reportez-vous à la WafLogBucketvariable dans la CloudFormation sortie. La figure suivante montre un exemple.

Capture d'écran illustrant un écran intitulé AWSWAFSecurity Automations et répertoriant quatre sorties



Si vous modifiez et remplacez le `<stack_name>-waf_log_conf.json` fichier sur Amazon S3, la fonction `Log Parser` Lambda prend en compte les nouvelles valeurs lors du traitement des nouveaux fichiers journaux AWS WAF. Voici un exemple de fichier de configuration :

Capture d'écran d'un exemple de fichier de configuration



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

Les paramètres incluent les suivants :

- Général :
  - Seuil de demandes (obligatoire) : nombre maximal de demandes acceptables toutes les cinq minutes, par adresse IP. Cette solution utilise la valeur que vous définissez lors du provisionnement ou de la mise à jour de la CloudFormation pile.
  - Période de blocage (obligatoire) - Période (en minutes) pour bloquer les adresses IP applicables. Cette solution utilise la valeur que vous définissez lors du provisionnement ou de la mise à jour de la CloudFormation pile.
  - Suffixes ignorés : les demandes accédant à ce type de ressource ne sont pas prises en compte dans le calcul du seuil de demande. Par défaut, cette liste est vide.
- Liste d'URI - Utilisez-la pour définir un seuil de demande personnalisé et une période de blocage pour des raisons spécifiques. URLs Par défaut, cette liste est vide.

Lorsque les journaux WAF arrivent dans le WafLogBucket, ils sont traités par la fonction d'analyse de journaux Lambda en utilisant les configurations de votre fichier de configuration. La solution écrit le résultat dans un fichier de sortie nommé `<stack_name>-waf_log_out.json` dans le même compartiment. Si le fichier de sortie contient une liste des adresses IP identifiées comme des attaquants, la solution les ajoute à l'adresse IP WAF définie pour HTTP Flood, et l'accès à votre

application est bloqué. Si les fichiers de sortie n'ont pas d'adresse IP, vérifiez si votre fichier de configuration est valide ou si la limite de débit est dépassée selon le fichier de configuration.

Utiliser le fichier JSON de l'analyseur de journal Lambda pour protéger les scanners et les sondes

Si vous avez choisi `Yes - AWS Lambda log parser` le paramètre du modèle Activate Scanner & Probe Protection, cette solution crée un fichier de configuration nommé `<stack_name>-app_log_conf.json` et le télécharge dans le compartiment Amazon S3 défini utilisé pour stocker CloudFront les fichiers journaux de l'Application Load Balancer.

Si vous modifiez et remplacez sur Amazon S3, la `<stack_name>-app_log_conf.json` fonction `Log Parser` Lambda prend en compte les nouvelles valeurs lors du traitement des nouveaux fichiers journaux AWS WAF. Voici un exemple de fichier de configuration :

Capture d'écran du fichier de configuration

```
{
    "general": {
        "errorThreshold": 50,
        "blockPeriod": 240,
        "errorCodes": ["400", "401", "403", "404", "405"]
    },
    "uriList": {
        "/login": {
            "errorThreshold": 5,
            "blockPeriod": 600
        },
        "/api/feedback": {
            "errorThreshold": 10,
            "blockPeriod": 240
        }
    }
}
```

Les paramètres incluent les suivants :

- Général :
  - Seuil d'erreur (obligatoire) - Le nombre maximum de mauvaises demandes acceptables par minute, par adresse IP. Cette solution utilise la valeur que vous avez définie lors du provisionnement ou de la mise à jour de la CloudFormation pile.
  - Période de blocage (obligatoire) - Période (en minutes) pour bloquer les adresses IP applicables. Cette solution utilise la valeur que vous avez définie lors du provisionnement ou de la mise à jour de la CloudFormation pile.

- Codes d'erreur : le code d'état renvoyé est considéré comme une erreur. Par défaut, la liste considère les codes d'état HTTP suivants comme des erreurs : `400 (Bad Request)401 (Unauthorized)`,`403 (Forbidden)`,`404 (Not Found)`, et`405 (Method Not Allowed)`.
- Liste d'URI - Utilisez-la pour définir un seuil de demande personnalisé et une période de blocage pour des raisons spécifiques URLs. Par défaut, cette liste est vide.

Lorsque les journaux d'accès aux applications arrivent dans le AppAccessLogBucket, la fonction `Log Parser` Lambda les traite en utilisant les configurations de votre fichier de configuration. La solution écrit le résultat dans un fichier de sortie nommé `<stack_name>`-app_log_out.json` dans le même compartiment. Si le fichier de sortie contient une liste des adresses IP identifiées comme des attaquants, la solution les ajoute à l'adresse IP WAF définie pour Scanner & Probe et les empêche d'accéder à votre application. Si les fichiers de sortie n'ont pas d'adresse IP, vérifiez si votre fichier de configuration est valide ou si la limite de débit a été dépassée conformément au fichier de configuration.

Utiliser le pays et l'URI dans l'analyseur de log Athena HTTP flood

Vous pouvez les regrouper par IPs pays et par URI dans la requête Athena afin de détecter et de bloquer les attaques HTTP Flood dont les modèles d'URI sont imprévisibles. Pour ce faire, sélectionnez l'une des options (`Country`,`URI`,`Country and URI`) pour le paramètre de requête Group By Requests in HTTP Flood Athena Query lors du lancement de la pile.

Vous pouvez également saisir un seuil de demande par pays à l'aide du paramètre Seuil de demande par pays. Par exemple, `{"TR": 50,"ER":150}`. La solution utilise ces seuils pour les demandes provenant de ces pays spécifiés. La solution utilise le seuil par défaut pour les demandes provenant d'autres pays.

> **Note**
>
> Si vous définissez un seuil par pays, la solution inclut automatiquement le pays dans la clause de regroupement par requête Athena. Pour plus d'informations, consultez le tableau des paramètres à l'étape 1. Lancez la pile.

La solution compte le seuil de demande sur une période de cinq minutes par défaut. Ceci est configurable avec le paramètre Athena Query Run Time Schedule (Minute).

> **Note**
>
> La requête Athena calcule le seuil par minute en divisant le seuil de demande par la période. Par exemple :
> Seuil de demande (seuil par défaut ou seuil par pays) : 100
> Durée d'exécution d'Athena Query : 5
> Seuil de demande par minute : 20 = 100/5

Afficher les requêtes Amazon Athena

Si vous avez sélectionné `Yes - Amazon Athena log parser` les paramètres du modèle Activate HTTP Flood Protection ou Activate Scanner & Probe Protection, cette solution crée et exécute des requêtes Athena pour les journaux ALB (`ScannersProbesLogParser`) CloudFront ou AWS WAF (`HTTPFloodLogParser`), analyse la sortie et met à jour AWS WAF en conséquence.

Pour améliorer les performances et réduire les coûts, la solution partitionne les journaux en fonction des horodatages figurant dans les noms de fichiers. La solution génère dynamiquement des requêtes Athena pour utiliser des clés de partition (année, mois, jour et heure). Par défaut, les requêtes sont exécutées toutes les cinq minutes. Vous pouvez configurer leurs programmes d'exécution en modifiant la valeur du paramètre du modèle Athena Query Run Time Schedule (Minute). Chaque exécution de requête analyse les données des quatre à cinq dernières heures par défaut. Vous pouvez configurer la quantité de données qu'une requête analyse en modifiant la valeur du paramètre du modèle WAF Block Period. La solution place également les requêtes dans des groupes de travail distincts afin de gérer l'accès aux requêtes et les coûts.

> **Note**
>
> Vérifiez qu'Athena est configurée pour accéder au catalogue de données AWS Glue. Cette solution crée le catalogue de données des journaux d'accès dans AWS Glue et configure une requête Athena pour traiter les données. Si Athena n'est pas correctement configurée, la requête ne s'exécute pas. Pour plus d'informations, reportez-vous à la section Mise à niveau vers le dernier catalogue de données AWSAWS Glue step-by-step.

Pour consulter ces requêtes, procédez comme suit :

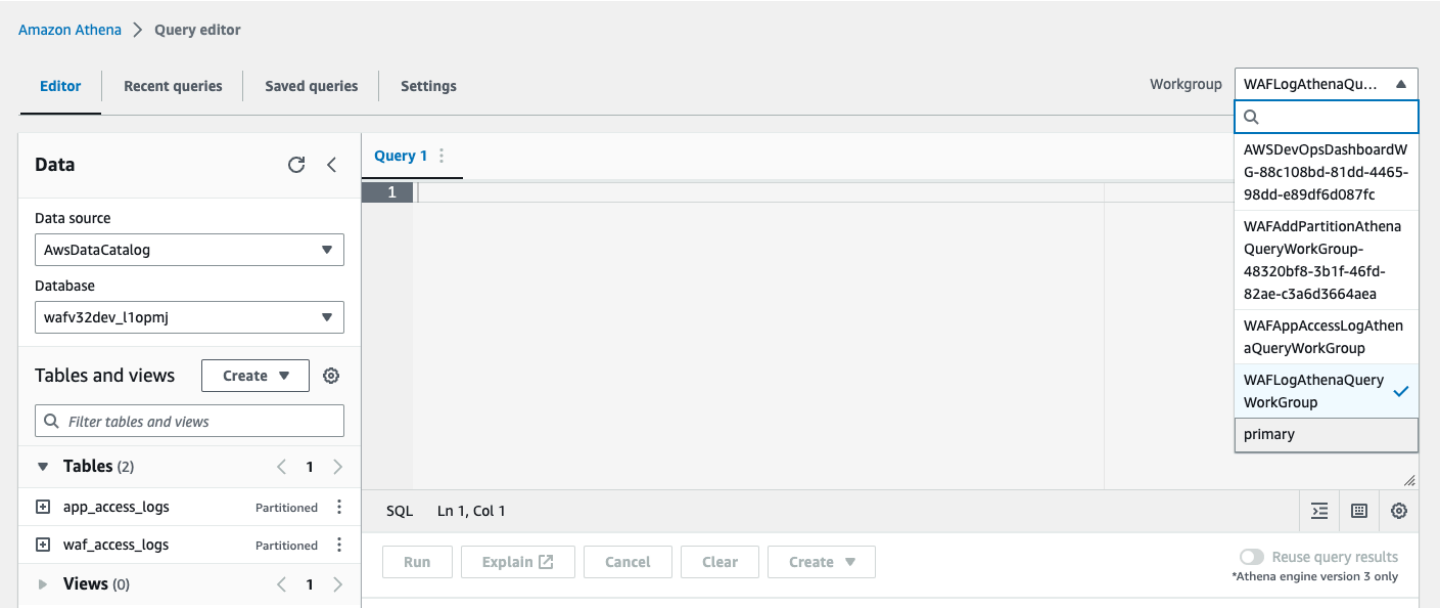
Afficher les requêtes du journal WAF

1. Connectez-vous à la console Amazon Athena.
2. Choisissez Lancer l'éditeur de requête.
3. Sélectionnez la base de données pour cette solution.
4. Sélectionnez WAFLogAthenaQueryWorkGroupdans la liste déroulante.

> **Note**
>
> Ce groupe de travail n'existe que si vous avez sélectionné le paramètre `Yes - Amazon Athena log parser` de modèle Activate HTTP Flood Protection.

5. Choisissez Switch pour changer de groupe de travail.

Capture d'écran de l'éditeur de requêtes Athena ne montrant aucune requête



1. Sélectionnez l'onglet Historique.
2. Sélectionnez et ouvrez `SELECT` des requêtes dans la liste.

Afficher les requêtes du journal d'accès aux applications

1. Connectez-vous à la console Amazon Athena.

2. Sélectionnez l'onglet Groupe de travail.
3. Sélectionnez WAFAppAccessLogAthenaQueryWorkGroupdans la liste.

> **Note**
>
> Ce groupe de travail n'existe que si vous avez sélectionné le paramètre `Yes - Amazon Athena log parser` de modèle Activate Scanner & Probe Protection.

4. Choisissez Switch workgroup.
5. Sélectionnez l'onglet Requêtes récentes.
6. Sélectionnez et ouvrez `SELECT` des requêtes dans la liste.

Afficher l'ajout de requêtes de partition Athena

1. Connectez-vous à la console Amazon Athena.
2. Sélectionnez l'onglet Groupe de travail.
3. Sélectionnez WAFAddPartitionAthenaQueryWorkGroupdans la liste.

> **Note**
>
> Ce groupe de travail existe uniquement si vous avez sélectionné le paramètre `Yes - Amazon Athena log parser` de modèle Activate HTTP Flood Protection and/or Activate Scanner & Probe Protection.

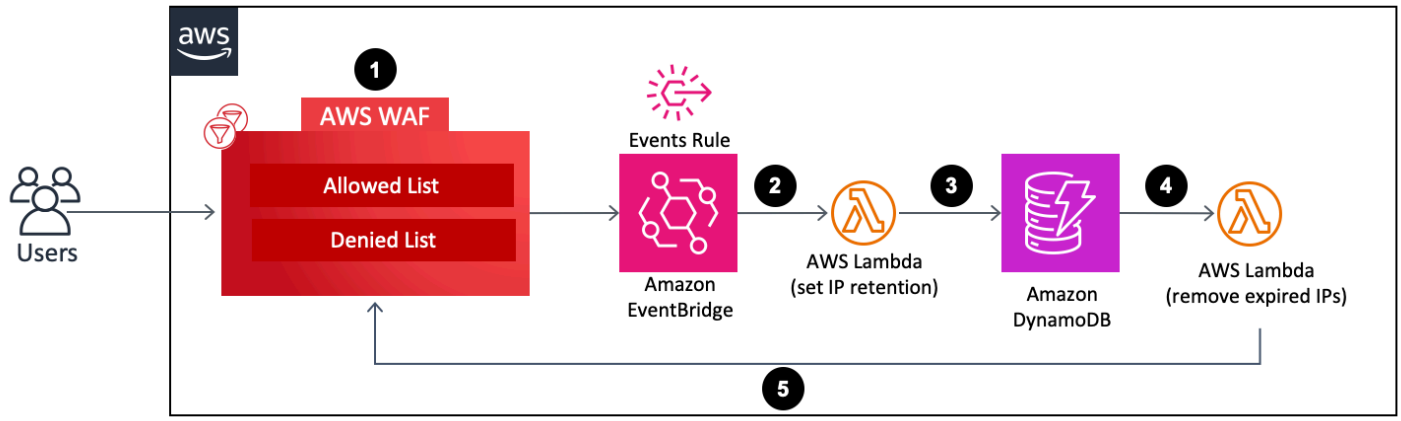
4. Sélectionnez Changer de groupe de travail.
5. Sélectionnez l'onglet Historique.
6. Sélectionnez et ouvrez `ALTER TABLE` des requêtes dans la liste. Ces requêtes sont exécutées toutes les heures pour ajouter une nouvelle partition horaire à la table Athena.

Configuration de la rétention des adresses IP sur les ensembles d'adresses IP AWS WAF autorisés et refusés

Vous pouvez configurer la rétention des adresses IP sur les ensembles d'adresses IP AWS WAF autorisés et refusés créés par la solution. Les sections suivantes expliquent son fonctionnement et indiquent les étapes à suivre pour le configurer.

Comment ça marche

Schéma d'architecture illustrant les listes d'autorisations et de refus d'AWS WAF et les autres ressources AWS



1. Lorsqu'un utilisateur met à jour (ajoute ou supprime une adresse IP) l'ensemble d'adresses IP WAF autorisées ou refusées, cette action appelle un appel d'API AWS `UpdateIPSet` WAF et crée un événement.
2. Une règle Amazon EventBridge Events détecte les événements sur la base d'un modèle d'événement prédéfini et invoque une fonction Lambda pour définir la période de conservation de toutes les adresses IP présentes dans l'ensemble d'adresses IP après la mise à jour.
3. La fonction Lambda traite les événements, extrait les données pertinentes pour la conservation des adresses IP (telles que le nom de l'ensemble d'adresses IP, l'ID, l'étendue, les adresses IP) et les insère dans une table DynamoDB. Il insère également un `ExpirationTime` attribut pour chaque élément DynamoDB. La solution calcule le délai d'expiration en ajoutant une période de rétention définie par l'utilisateur à l'heure de l'événement. DynamoDB Streams et Time to Live (TTL) sont activés dans la table. L'attribut TTL est`ExpirationTime`.
4. Lorsqu'un élément atteint son délai d'expiration, le protocole TTL est invoqué et DynamoDB le supprime de la table après son délai d'expiration. Lors de la suppression de l'élément, celui-ci est ajouté au flux DynamoDB, qui invoque une fonction Lambda pour le traitement en aval.
5. La fonction Lambda obtient les informations relatives à l'élément supprimé à partir du flux DynamoDB et lance un appel d'API AWS WAF pour supprimer les adresses IP expirées incluses dans l'élément de l'ensemble d'adresses IP AWS WAF cible.

Activer la conservation des adresses IP

Pour activer la conservation des adresses IP, procédez comme suit :

1. Dans la pile Cloudformation que vous déployez ou mettez à jour, entrez la période de rétention IP (minutes) pour l'ensemble d'adresses IP autorisé et la période de rétention IP (minutes) pour l'ensemble d'adresses IP refusées. La durée de conservation minimale est de 15 minutes. La solution traite n'importe quel nombre compris entre `0` et `15` comme`15`. Pour plus d'informations sur la configuration du déploiement, reportez-vous à l'étape 1. Lancez la pile.
2. Entrez une adresse e-mail si vous souhaitez recevoir une notification par e-mail lorsque des adresses IP expirées sont supprimées de l'ensemble d'adresses IP AWS WAF. Si vous choisissez de recevoir une notification par e-mail, vous devez confirmer votre inscription à l'aide du lien figurant dans l'e-mail que vous recevrez une fois la solution déployée avec succès. Pour plus d'informations sur la configuration du déploiement, reportez-vous à l'étape 1. Lancez la pile.
3. Mettez à jour l'ensemble d'adresses IP AWS WAF en ajoutant ou en supprimant des adresses IP. Cela lance le processus de conservation des adresses IP et crée un élément DynamoDB, y compris une liste d'expiration des adresses IP. Cette liste d'expiration comprend les adresses IP qui existent dans l'ensemble d'adresses IP AWS WAF après sa mise à jour.
4. Une fois que l'élément DynamoDB a atteint son délai d'expiration et est supprimé du tableau, la solution supprime les adresses IP incluses dans la liste d'expiration des adresses IP de l'élément de l'ensemble d'adresses IP WAF.

> **Note**
>
> En fonction de l'heure à laquelle DynamoDB supprime un élément expiré par TTL, l'opération de suppression effective d'une adresse IP expirée de l'ensemble d'adresses IP AWS WAF peut varier. La suppression TTL DynamoDB dépend principalement de la taille et du niveau d'activité d'une table. Attendez-vous à un retard dans l'opération de suppression d'AWS WAF en raison du retard potentiel de l'opération de suppression DynamoDB. En général, la solution supprime les adresses IP expirées de l'ensemble d'adresses IP AWS WAF peu de temps après la suppression TTL de DynamoDB. Pour plus d'informations, reportez-vous à DynamoDB Time to Live (TTL) dans le manuel du développeur Amazon DynamoDB.

Créez un tableau de bord de surveillance

AWS vous recommande de configurer un système de surveillance de base personnalisé pour chaque point de terminaison critique. Pour plus d'informations sur la création et l'utilisation de vues métriques personnalisées, consultez CloudWatch Tableaux de bord - Création et utilisation de vues de mesures personnalisées et Utilisation des CloudWatch tableaux de bord Amazon.

La capture d'écran du tableau de bord suivante montre un exemple de système de surveillance de base personnalisé.

capture d'écran du CloudFront tableau de bord

Le tableau de bord affiche les statistiques suivantes :

- Demandes autorisées ou bloquées : indique si vous recevez une augmentation des accès autorisés (deux fois le pic d'accès normal) ou des accès bloqués (toute période identifiant plus de 1 000 demandes bloquées). CloudWatch envoie une alerte à une chaîne Slack. Vous pouvez utiliser cette métrique pour suivre les attaques DDo S connues (lorsque le nombre de demandes bloquées augmente) ou une nouvelle version d'une attaque (lorsque les demandes sont autorisées à accéder au système).

> **Note**
>
> Remarque : La solution fournit cette métrique.

- BytesDownloaded vs Uploaded : permet d'identifier les cas où une attaque DDo S cible un service qui ne reçoit normalement pas beaucoup d'accès pour épuiser des ressources (par exemple, un composant du moteur de recherche envoie MBs des informations pour un ensemble de paramètres de demande spécifique).
- Effet de propagation de l'ELB et longueur de la file d'attente : permettent de vérifier si une attaque DDo S endommage l'infrastructure et si l'attaquant contourne la couche CloudFront AWS WAF et attaque directement des ressources non protégées.
- Nombre de demandes ELB : aide à identifier les dommages causés à l'infrastructure. Cette métrique indique si l'attaquant contourne la couche de protection ou si vous devez revoir une règle de CloudFront cache pour augmenter le taux de réussite du cache.
- ELB Healthy Host - Vous pouvez l'utiliser comme autre métrique de vérification de l'état du système.
- Utilisation du processeur ASG : permet d'identifier si l'attaquant contourne AWS WAF CloudFront et Elastic Load Balancing. Vous pouvez également utiliser cette métrique pour identifier les dégâts d'une attaque.

Gérer les faux positifs XSS

Cette solution configure une règle AWS WAF qui inspecte les éléments fréquemment explorés des demandes entrantes afin d'identifier et de bloquer les attaques XSS. Ce modèle de détection est moins efficace si votre charge de travail permet à des utilisateurs légitimes de composer et de soumettre du code HTML, par exemple à l'aide d'un éditeur de texte enrichi dans un système de gestion de contenu. Dans ce scénario, envisagez de créer une règle d'exception qui contourne la règle XSS par défaut pour les modèles d'URL spécifiques qui acceptent la saisie de texte enrichi, et de mettre en œuvre d'autres mécanismes pour protéger les personnes exclues. URLs

En outre, certains formats d'image ou de données personnalisés peuvent générer des faux positifs car ils contiennent des modèles indiquant une attaque XSS potentielle dans le contenu HTML. Par exemple, un fichier SVG peut contenir une `<script>` balise. Si vous attendez ce type de contenu de la part d'utilisateurs légitimes, adaptez étroitement vos règles XSS pour autoriser les requêtes HTML qui incluent ces autres formats de données.

Procédez comme suit pour mettre à jour la règle XSS afin d'exclure ceux URLs qui acceptent le HTML en entrée. Reportez-vous au manuel Amazon WAF Developer Guide pour obtenir des instructions détaillées.

1. Connectez-vous à la console AWS WAF.
2. Créez une correspondance de chaîne ou une condition regex.
3. Configurez les paramètres du filtre pour inspecter les valeurs d'URI et de liste que vous souhaitez accepter par rapport à la règle XSS.
4. Modifiez la règle XSS de cette solution et ajoutez la nouvelle condition que vous avez créée.

   Par exemple, pour exclure tous les éléments URLs de la liste, choisissez ce qui suit pour Lorsqu'une demande est envoyée :

   - ne
   - correspondre à au moins un des filtres dans la condition de correspondance des chaînes
   - Liste des autorisations XSS

Résolution des problèmes

Si vous avez besoin d'aide avec cette solution, contactez le Support pour ouvrir un dossier d'assistance pour cette solution.

Contacter AWS Support

Si vous disposez d'AWS Business Support+, d'AWS Enterprise Support ou d'Unified Operations, vous pouvez utiliser le centre de support AWS pour obtenir l'assistance d'experts concernant cette solution. Les sections suivantes fournissent des instructions.

Créer un dossier

1. Ouvrez le Centre de support.
2. Choisissez Create case (Créer une demande).

Comment pouvons-nous vous aider ?

1. Choisissez Technique.
2. Dans le champ Service, sélectionnez Solutions.
3. Dans Catégorie, sélectionnez Automatisations de sécurité pour AWS WAF.
4. Pour Severity, l'option qui correspond le mieux à votre cas d'utilisation.
5. Lorsque vous entrez le service, la catégorie et la gravité, l'interface contient des liens vers des questions de dépannage courantes. Si vous ne parvenez pas à résoudre votre question à l'aide de ces liens, sélectionnez Étape suivante : Informations supplémentaires.

Informations supplémentaires

1. Dans le champ Objet, saisissez un texte résumant votre question ou problème.
2. Pour la description, décrivez le problème en détail, y compris le nom de cette solution et la version que vous utilisez, par exemple : Security Automations for AWS WAF Vx.y.z.
3. Choisissez Joindre des fichiers.
4. Joignez les informations dont le Support a besoin pour traiter la demande.

Aidez-nous à résoudre votre cas plus rapidement

1. Entrez les informations demandées.
2. Cliquez sur Étape suivante : résoudre maintenant ou nous contacter.

Résolvez maintenant ou contactez-nous

1. Passez en revue les solutions Solve now.
2. Si vous ne parvenez pas à résoudre votre problème avec ces solutions, choisissez Contactez-nous, entrez les informations demandées, puis cliquez sur Soumettre.

Manuel du développeur

Cette section fournit le code source de la solution.

Code source

Consultez notre GitHub référentiel pour télécharger les modèles et les scripts de cette solution et pour partager vos personnalisations avec d'autres utilisateurs.

Les modèles de cette solution sont générés à l'aide du kit AWS CDK. Reportez-vous au fichier README.md pour plus d'informations.

Référence

Cette section inclut des informations sur une fonctionnalité facultative permettant de collecter des métriques uniques pour cette solution, des pointeurs vers des ressources connexes et une liste des créateurs qui ont contribué à cette solution.

Collecte de données anonymisée

Cette solution inclut une option permettant d'envoyer des métriques opérationnelles à AWS. Nous utilisons ces données pour mieux comprendre la façon dont les clients utilisent cette solution et les services et produits associés. Lorsqu'elle est activée, la solution collecte les informations suivantes et les envoie à AWS lors du déploiement initial du CloudFormation modèle :

- ID de solution : identifiant de solution AWS
- ID unique (UUID) : identifiant unique généré aléatoirement pour chaque déploiement de cette solution
- Horodatage - Horodatage de la collecte de données
- Configuration de la solution : fonctionnalités activées et paramètres définis lors du lancement initial
- Cycle de vie : durée pendant laquelle le client a utilisé cette solution (sur la base de la suppression des piles)
- Enregistrez les données de l'analyseur syntaxique :
  - Le nombre d'adresses IP comprises dans le set IP Scanner & Probe, le set Bad Bot IP et l'IP HTTP Flood paramétré pour bloquer
  - Le nombre de demandes traitées et bloquées
- IP répertorie les données de l'analyseur :
  - Le nombre d'adresses IP dans l'ensemble d'adresses IP des listes de réputation
  - Le nombre de demandes traitées et bloquées
- Données de conservation des adresses IP : nombre d'adresses IP expirées supprimées de l'ensemble d'adresses IP autorisées ou refusées

AWS est propriétaire des données collectées dans le cadre de cette enquête. La collecte de données est soumise à la politique de confidentialité d'AWS. Pour désactiver cette fonctionnalité, suivez les étapes ci-dessous avant de lancer le CloudFormation modèle AWS.

1. Téléchargez l'`aws-waf-security-automations.template`AWS CloudFormation sur votre disque dur local.
2. Ouvrez le CloudFormation modèle dans un éditeur de texte.
3. Modifiez la section de mappage du CloudFormation modèle à partir de :

```
Solution:
  Data:
   SendAnonymizedUsageData: "Yes"
```

   par :

```
Solution:
  Data:
   SendAnonymizedUsageData: "No"
```

4. Connectez-vous à la CloudFormation console AWS.
5. Sélectionnez Créer une pile.
6. Sur la page Créer une pile, section Spécifier le modèle, sélectionnez Télécharger un fichier modèle.
7. Sous Télécharger un fichier modèle, choisissez Choisir un fichier et sélectionnez le modèle modifié sur votre disque local.
8. Choisissez Next et suivez les étapes de l'étape 1. Lancez la pile.

Ressources connexes

Livres blancs AWS associés

- Bonnes pratiques AWS pour la résilience DDo des systèmes

Articles de blog relatifs à la sécurité AWS associés

- Comment empêcher les hotlinking à l'aide d'AWS WAF, CloudFront Amazon et Referer Checking

Listes de réputation IP de tiers

- Site web de Spamhaus DROP List
- Liste des adresses IP des menaces émergentes de Proofpoint
- Liste des nœuds de sortie de Tor

Collaborateurs

- Héitor Vital
- Lee Atkinson
- Ben Potter
- Vlad Vlasceanu
- Aijun Peng
- Chaitanya Deolankar
- Shu Jackson
- William Quan
- Mykhailo Markhain

Révisions

Consultez le fichier ChangeLog.md dans notre GitHub référentiel pour suivre les améliorations et les correctifs spécifiques à chaque version.

Avis

Ce guide de mise en œuvre est fourni à titre informatif uniquement. Il représente les offres de produits et les pratiques actuelles d'AWS à la date de publication de ce document, qui sont susceptibles d'être modifiées sans préavis. Les clients sont tenus de procéder à leur propre évaluation indépendante des informations contenues dans ce document et de toute utilisation des produits ou services AWS, chacun étant fourni « tel quel » sans garantie d'aucune sorte, expresse ou implicite. Ce document ne crée aucune garantie, représentation, engagement contractuel, condition ou assurance de la part d'AWS, de ses filiales, fournisseurs ou concédants de licence. Les responsabilités et obligations d'AWS vis-à-vis de ses clients sont régies par les contrats AWS. Le présent document ne fait partie d'aucun, et ne modifie aucun, contrat entre AWS et ses clients.

La solution Security Automations for AWS WAF est concédée sous licence selon les termes de la licence Apache version 2.0.

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.