Guide de mise en œuvre

Automatisations de sécurité pour AWS WAF

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

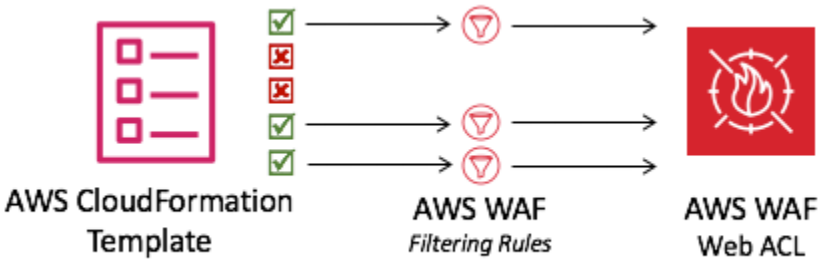
Table of Contents

Déployez automatiquement une liste de contrôle d'accès Web unique qui filtre les attaques Web avec Security Automations sur AWS WAF

Date de publication : septembre 2016 (dernière mise à jour : décembre 2024)

La AWS WAF solution Security Automations for déploie un ensemble de règles préconfigurées pour vous aider à protéger vos applications contre les exploits Web courants. Le service principal de cette solution permet de 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. AWS WAF Vous pouvez l'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 AWS des ressources telles qu'Amazon CloudFront, Application Load Balancer (ALB) et Amazon API Gateway. Pour plus d'informations sur les types de ressources pris AWS WAFen charge, consultez le AWS WAF AWS Firewall Manager, et le Guide AWS Shield Advanced du développeur.

La configuration des AWS WAF règles peut être 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 AWS WAF solution Security Automations for déploie automatiquement une seule liste de contrôle d'accès Web (ACL) avec un ensemble de AWS WAF règles conçues pour filtrer les attaques Web courantes. Lors de la configuration initiale du AWS CloudFormationmodèle 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 leur (s) CloudFront distribution (s) existante ALB (s) et les bloque le cas échéant.



Configuration du AWS WAF Web ACL

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 AWS sécurité, de calcul, de stockage et autres nécessaires au déploiement de cette solution AWS, en utilisant les AWS meilleures pratiques en matière de sécurité et de disponibilité.

Les informations contenues dans ce guide supposent une connaissance pratique de AWS services tels que 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**
>
> À partir de la version 3.0.0, cette solution prend en charge la dernière version du AWS WAF service API (AWS WAF V2).

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 recommandons d'utiliser cette solution comme point de départ pour la mise en œuvre AWS WAF des règles. Vous pouvez personnaliser le code source, ajouter de nouvelles règles personnalisées et tirer parti de règles mieux AWS WAF gérées 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	Coût

Si tu veux...	Lisez.
la quantité de données ingérées, stockées et traitées.	
Comprenez les considérations de sécurité liées à cette solution.	Sécurité
Découvrez ceux qui Régions AWS sont pris en charge pour cette solution.	Soutenu Régions AWS
Consultez ou téléchargez le CloudFormation modèle inclus dans cette solution pour déployer automatiquement les ressources d'infrast ructure (la « pile ») de cette solution.	AWS CloudFormation modèle
Support À utiliser pour vous aider à déployer, à utiliser ou à dépanner la solution.	Support
Accédez au code source et utilisez éventuell ement le AWS Cloud Development Kit (AWS CDK) pour déployer la solution	GitHubréférentiel

Fonctionnalités et avantages

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

Sécurisez vos applications Web à l'aide de groupes de AWS Managed Rules règles

AWS Managed Rules pour AWS WAF 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 AWS gérés, des groupes de règles de base AWSAWS gérés et des groupes de règles spécifiques à des cas d'utilisation gérés. Vous avez la possibilité de sélectionner un ou plusieurs groupes de règles pour votre site WebACL, dans la limite du quota d'unités de ACL capacité Web (WCU) maximum.

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

La règle personnalisée HTTPFlood 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 :

- AWS WAF règle basée sur le taux
- 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 empêcher d'atteindre le quota requis par les règles AWS WAF basées sur les taux. 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 permet d'identifier et de bloquer les HTTP inondations dont le URI schéma est imprévisible. Pour plus d'informations, reportez-vous aux sections Pays d'utilisation et URI in HTTP Flood Athena log parser.

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 Don'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.

Intégration à Service Catalog AppRegistry et au gestionnaire AWS d'applications Systems Manager

Cette solution inclut une AppRegistry ressource Service Catalog pour enregistrer le CloudFormation modèle de la solution et ses ressources sous-jacentes en tant qu'application à la fois dans AWS Service Catalog AppRegistry et dans AWS Systems Manager Application Manager. Grâce à cette intégration, vous pouvez gérer de manière centralisée les ressources de la solution.

Cas d’utilisation

Date de publication : septembre 2016 (dernière mise à jour : mai 2023)

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 AWS WAF règles

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

Personnalisez la protection HTTP contre les inondations de la couche 7

Cette solution propose trois options pour activer la protection HTTP contre les inondations. Vous pouvez sélectionner l'option qui répond à vos besoins pour vous protéger contre les DDoS attaques. Pour plus d'informations, voir Fournir une protection contre les inondations de couche 7 avec une règle personnalisée prédéfinie HTTP contre les inondations 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 de la manière d'utiliser AWS WAF et d'autres services pour créer des automatisations de sécurité sur le AWS Cloud. 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.

ALB Journaux

Cette solution utilise des journaux pour la ALB ressource. 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 basé sur des frameworks open source et prenant en charge les formats de fichier et de table ouverts. Cette solution exécute une requête Athena planifiée pour inspecter AWS WAF ou ALB enregistre si l'utilisateur le souhaite

`yes – Amazon Athena log parser` lors de l'activation de la règle de protection contre les HTTPinondations ou de la règle de protection contre les scanners et les sondes. CloudFront

AWS WAF règle

Une AWS WAF règle définit :

- Comment inspecter les HTTP (S) requêtes Web
- 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'un site WebACL.

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 AWS des ressources.

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 Lamba lance une inspection ou ALB enregistre si l'utilisateur le souhaite `yes – AWS Lambda log parser` lors de AWS WAF l'activation de la règle de protection contre les HTTPinondations ou de la règle de protection contre les scanners et les sondes. CloudFront

Groupes de règles gérés

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

type de ressource/point de terminaison

Vous pouvez associer AWS des ressources ACLs au Web pour les protéger. Ces ressources sont les ressources API Gateway CloudFront ALB AWS AppSync, Amazon Cognito, AWS App Runner

et AWS Verified Access. Actuellement, cette solution est prise en charge par Amazon CloudFront etALB.

WAF Journaux

Cette solution utilise les journaux générés par AWS WAF pour les ressources associées au WebACL. La règle de protection contre les HTTP inondations de cette solution inspecte ces journaux.

WCU

AWS WAF utilise les unités de capacité de la liste de contrôle d'accès Web (WCUs) () pour calculer et contrôler les ressources opérationnelles nécessaires à l'exécution de vos règles, de vos groupes de règles et du WebACLs. ACL AWS WAF applique des WCU quotas lorsque vous configurez vos groupes de règles et votre site WebACLs. WCUsn'affectent pas la façon dont le trafic AWS WAF Web est inspecté.

web ACL

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

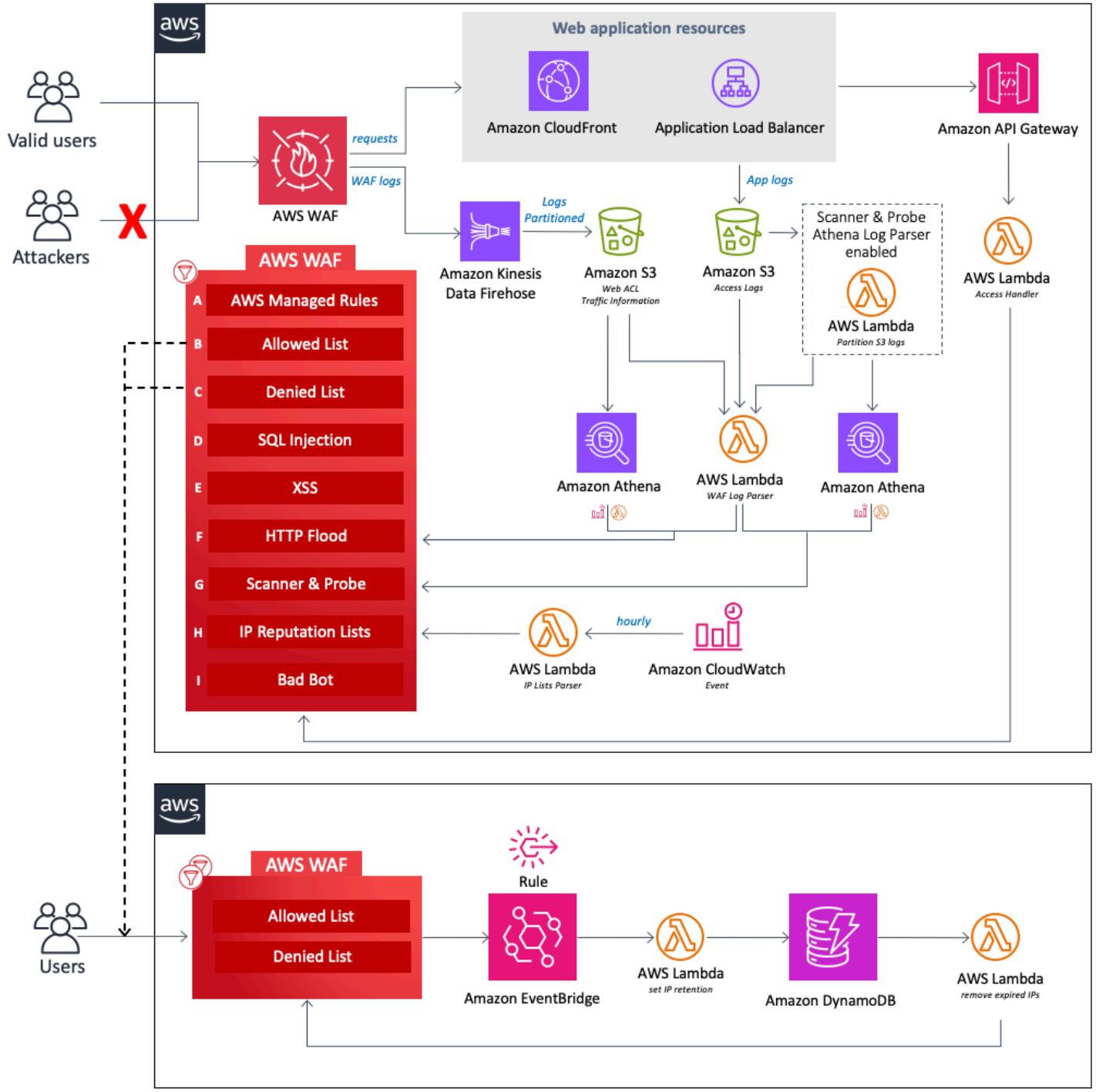
> **Note**
>
> Pour une référence générale des AWS termes, consultez le AWS glossaire.

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.



Automatisations de sécurité pour AWS WAF l'architecture sur AWS

Au cœur de la conception se trouve un AWS WAFsite WebACL, 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 au WebACL.

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 WAF règles.

- AWS Règles gérées (A) — Ce composant contient des groupes de règles de réputation AWS Managed Rules IP, 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 OWASPpublications, sans avoir à rédiger vos propres règles.
- Listes d'adresses IP manuelles (B et C) : ces composants créent deux AWS WAF règles. 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' AWS WAF adresses IP autorisées et refusées.
- SQLInjection (D) et XSS (E) : ces composants configurent deux AWS WAF règles conçues pour protéger contre les modèles courants SQL d'injection ou de script intersite (XSS) dans la URI chaîne de requête ou le corps d'une demande.
- HTTPFlood (F) — Ce composant protège contre les attaques consistant en un grand nombre de requêtes provenant d'une adresse IP particulière, telles qu'une DDoS attaque de couche Web 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 AWS WAF basée sur le taux ou en traitant les AWS WAF journaux 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 HTTP inondations, reportez-vous à la section Options de l'analyseur 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 Don'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 met automatiquement en place un honeypot, un mécanisme de sécurité destiné à attirer et à déjouer une tentative d'attaque. Le pot de miel de cette solution est un point de terminaison piège que vous pouvez insérer dans votre site Web pour détecter les demandes entrantes provenant des scrapeurs de contenu et des robots malveillants. Si une source accède au honeypot, la fonction `Access Handler` Lambda intercepte et inspecte la demande pour extraire son adresse IP, puis l'ajoute à une liste de blocage. AWS 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.

AWSConsidérations relatives à la conception de Well-Architected

Cette solution utilise les meilleures pratiques du 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, à Gateway, aux compartiments API Amazon S3 et aux autres composants de la solution.
- Nous développons, testons et publions la solution par le biais d'un AWS pipeline d'intégration et de livraison continues (CI/CD). 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 des services AWS sans serveur dans la mesure du possible (par exemple, Lambda, Firehose, GatewayAPI, 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 AWS services qui constituent cette solution ainsi que les détails de l'architecture sur la manière dont ces composants fonctionnent ensemble.

AWS services inclus dans cette solution

AWS service	Description	
AWS WAF	Noyau. Déploie un AWS WAF site WebACL, des groupes de AWS Managed Rules règles, des règles personnalisées et des ensembles d'adresse s IP. Passe AWS WAF API des appels pour bloquer les attaques courantes et sécuriser les applications Web.	
Amazon Data Firehose	Noyau. Fournit AWS WAF les journaux aux compartiments Amazon S3.	
Amazon S3	Noyau. AWS WAF CloudFron tMagasins et ALB journaux.	
AWS Lambda	Noyau. Déploie plusieurs fonctions Lambda pour prendre en charge les règles personnalisées.	
Amazon EventBridge	Noyau. Crée des règles d'événements pour appeler Lambda.	

AWS service	Description	
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.	
APIPasserelle Amazon	Soutenir. Crée un point de terminaison du bot honeypot défectueux.	
Amazon SNS	Soutenir. Envoie des notifications par e-mail à Amazon Simple Notification Service (AmazonSNS) pour favoriser la conservation 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 les protections contre les HTTP inondations et les protections par scanner et sonde. Les sections suivantes expliquent chacune de ces options plus en détail.

AWS WAF règle basée sur le taux

Des règles basées sur les taux 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 HTTPFlood 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 les résultats et de les 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 de règles AWS WAF basées sur les taux et que vous savez comment SQL implémenter des personnalisations. Pour plus d'informations sur la modification de la requête par défaut, consultez la section Afficher les requêtes Amazon Athena.

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

AWS Lambda analyseur de journaux

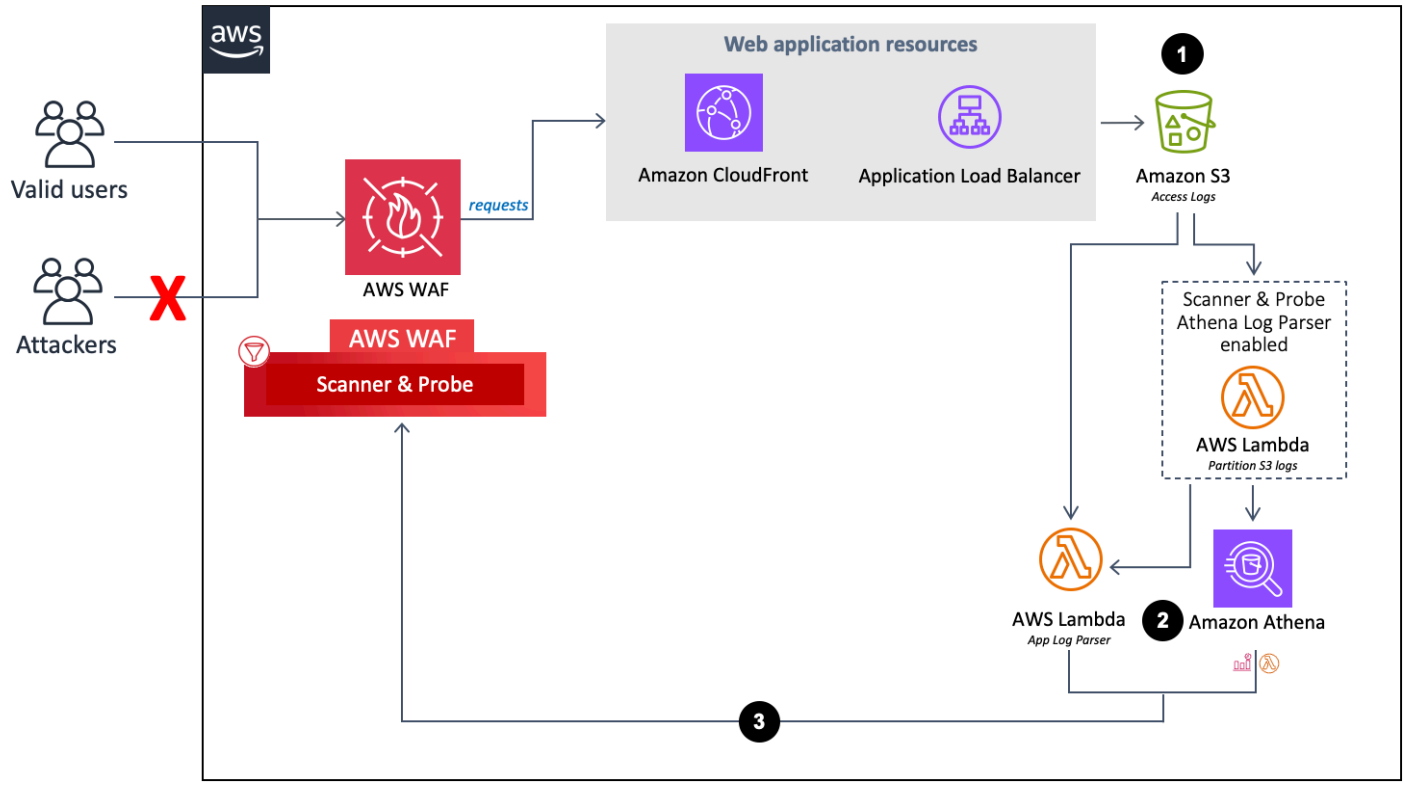
Les paramètres du modèle HTTPFlood Protection et Scanner & Probe Protection fournissent l'option AWS Lambda Log Parser. Utilisez l'analyseur de journaux Lambda uniquement lorsque la règle AWS WAF basée sur le taux et les options de l'analyseur de journaux Amazon Athena ne sont pas disponibles. L'une 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.

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 AWS WAF blocage. 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

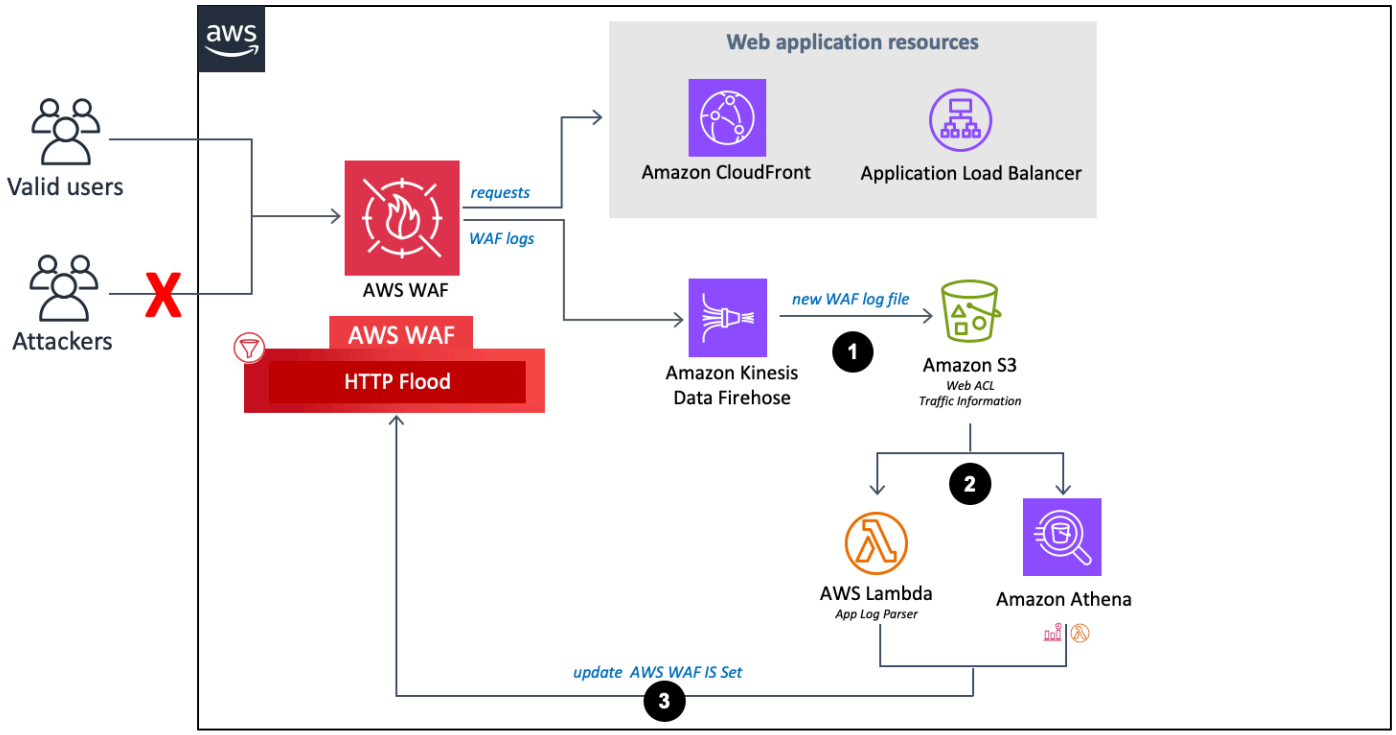
1. Lorsque CloudFront ou an ALB reçoit des demandes au nom de votre application Web, il envoie des journaux d'accès à un compartiment Amazon S3.
   a. (Facultatif) Si vous sélectionnez `Yes - Amazon Athena log parser` comme paramètres du modèle Activate HTTP Flood Protection et Activate Scanner & Probe Protection, une fonction Lambda déplace les journaux d'accès de leur dossier d'origine *<customer-bucket>*/`AWSLogs` vers un dossier nouvellement partitionné à leur *<customer-bucket>*/`AWSLogs-partitioned/`*<optional-prefix>* `/year=`*<YYYY>*`/month=`*<MM>* `/day=`*<DD>*`/hour=`*<HH>*`/` 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. Sur la base 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 la sortie est envoyée à. 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 AWS WAF IP 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 contre les HTTP inondations, cette solution fournit les composants suivants, qui analysent les AWS WAF journaux 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.



AWS WAF flux d'analyseur de journaux

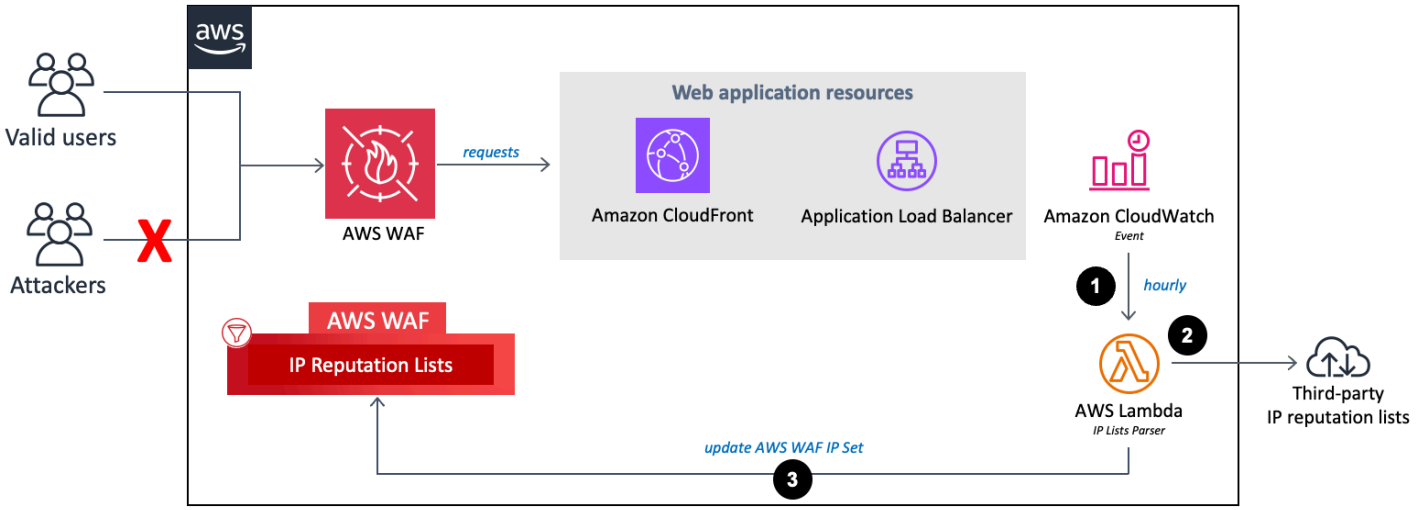
1. Lorsqu'il AWS WAF reçoit les journaux d'accès, il les envoie à un point de terminaison Firehose. Firehose envoie ensuite les journaux dans un compartiment partitionné dans Amazon S3 nommé *<customer-bucket>*/AWSLogs/ *<optional-prefix>*/year=*<YYYY>* /month=*<MM>*/ day=*<DD>*/hour= *<HH>*/
2. Sur la base 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 la sortie est redirigée 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 AWS WAF IP 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.

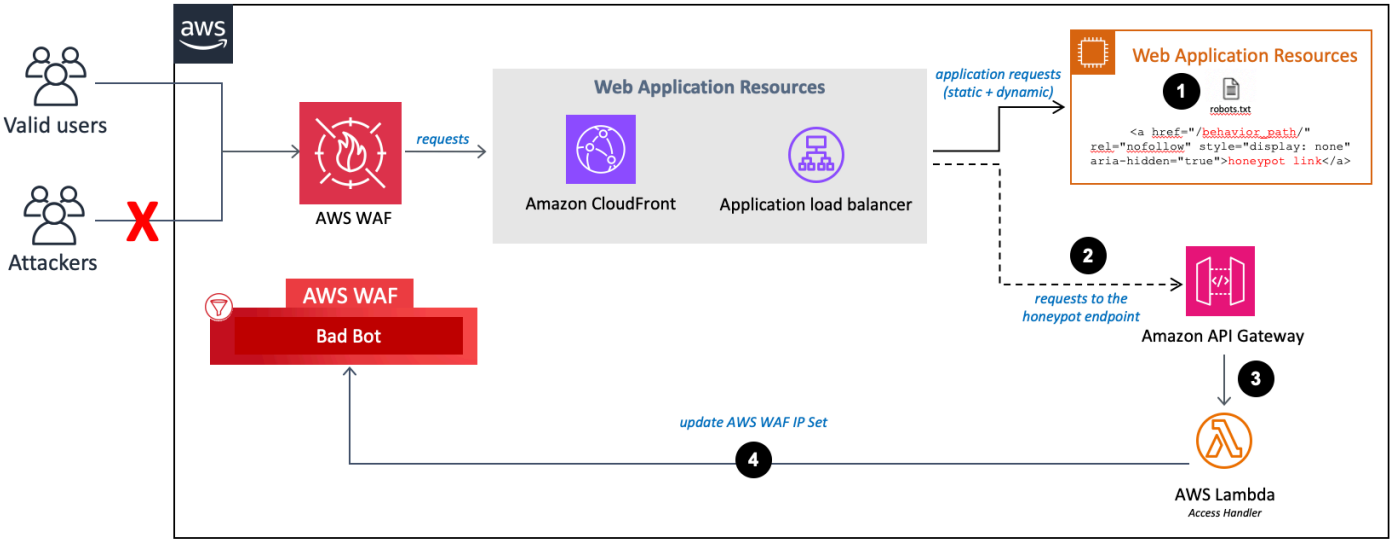


La réputation IP répertorie le flux de l'analyseur

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 :
   - Spamhaus DROP et listes EDROP
   - Liste IP des menaces émergentes de Proofpoint
   - Liste des nœuds de sortie de Tor
3. La fonction Lambda met à jour la liste de AWS WAF blocage avec les adresses IP actuelles.

Gestionnaire d'accès

La fonction `Access Handler` Lambda inspecte les requêtes adressées au point de terminaison Honeypot pour en extraire l'adresse IP source.



Gestionnaire d'accès et point de terminaison Honeypot

1. Intégrez le point de terminaison Honeypot à votre site Web et mettez à jour la norme d'exclusion de vos robots, comme décrit dans Intégrer le lien Honeypot dans votre application Web (facultatif).
2. Lorsqu'un scraper de contenu ou un bot malveillant accède au point de terminaison Honeypot, il invoque la `Access Handler` fonction Lambda.
3. 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.
4. La fonction Lambda met à jour une condition d'ensemble d' AWS WAF adresses IP pour bloquer ces adresses IP.

Planifiez votre déploiement

Cette section décrit le coût, la sécurité et les autres considérations à prendre en compte avant de déployer la solution. the section called “Quotas”

Soutenu Régions AWS

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 toutes disponibles Régions AWS. Par conséquent, vous devez lancer cette solution Région AWS là où ces services sont disponibles. Pour connaître la disponibilité la plus récente des AWS services par région, consultez la Région AWS liste complète des services.

	AWS WAF Web ACL	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 AWS Lambda journaux				✓
oui - Analyseur de journaux Amazon Athena		✓	✓	✓
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`).

Coût

Vous êtes responsable du coût des AWS services utilisés lors de l'exécution de la AWS WAF solution Security Automations for. 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 AWS Cost Explorerpour aider à gérer les coûts. Pour plus de détails, consultez la page Web de tarification de chaque AWS service 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 USA Est (Virginie du Nord) (à l'exception du niveau AWS gratuit). 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 AWS Lambda journaux pour la protection contre les HTTP inondations et de la protection contre les scanners et les sondes

AWS service	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 $

AWS service	Dimensions/mois	Coût [USD]
APIPasserelle Amazon	1 million de demandes	~3,40 $
AWS WAF web ACL	1	5,00$
AWS WAF règle	4	4,00$
AWS WAF demande	1 M	0,60$
Total		~23,60 $ 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 HTTP inondations et la protection contre les scanners et les sondes

AWS service	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, 7560 appels et durée moyenne de 500 millisecondes par exécution Lambda	~1,26 $
APIPasserelle Amazon	1 million de demandes	~3,40 $
Amazon Athena	1,2 million de visites CloudFront d'objets ou 1,2 million de ALB demandes par jour, ce qui génère un enregistrement journal	~4,32 $

AWS service	Dimensions/mois	Coût [USD]
	d'environ 500 octets par accès ou demande	
AWS WAF web ACL	1	5,00$
AWS WAF règle	4	4,00$
AWS WAF demande	1 M	0,60$
Total		~23,78 $ par mois

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

AWS service	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 de 500 millisecondes par exécution Lambda	~0,01 $
Amazon CloudWatch	Événements 2K	~0,00 $
AWS WAF Web ACL	1	5,00$
AWS WAF Règle	2	2,00$
WASWAFdemande	1 M	0,60$

AWS service	Dimensions/mois	Coût [USD]
Total		~7,61 $ par mois

Estimation du coût des CloudWatch grumes

Certains AWS services 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 aux journaux AWS WAF d'accès aux applications contenus dans 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 HTTPFlood Protection ou Scanner & Probe 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 WAFBlock 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 une AWS infrastructure, les responsabilités en matière de sécurité sont partagées entre vous et AWS. Ce modèle de responsabilité partagée réduit votre charge opérationnelle car il 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 AWS la sécurité, consultez AWS Cloud la section Sécurité.

Rôles IAM

Avec IAM les rôles, vous pouvez attribuer un accès, des politiques et des autorisations granulaires aux services et aux utilisateurs du AWS Cloud. Cette solution crée IAM des rôles 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 des AWS WAF règles, notamment des groupes de AWS Managed Rules règles et des règles personnalisées, afin de bloquer les attaques courantes suivantes :

- AWSRègles gérées : 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 AWS gérés, des groupes de règles de base AWS AWS gérés et des groupes de règles spécifiques à des cas d'utilisation gérés. Vous avez la possibilité de sélectionner un ou plusieurs groupes de règles pour votre site WebACL, dans la limite du quota d'unités de ACL capacité Web (WCU) maximum.
- SQLinjection — Les attaquants insèrent SQL du code malveillant dans les requêtes Web pour extraire des données de votre base de données. Nous avons conçu cette solution pour bloquer les requêtes Web contenant SQL du code potentiellement malveillant.
- XSS— Les attaquants utilisent les vulnérabilités d'un site Web bénin pour injecter des scripts malveillants destinés à un 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 XSS les attaques.
- HTTPinondations : les serveurs Web et les autres ressources dorsales sont exposés à des DDoS attaques, telles que des HTTP inondations. 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 AWS WAF journaux 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 à la recherche de 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 ou une requête Athena qui analyse CloudFront ou ALB accède automatiquement aux journaux, compte le nombre de demandes erronées provenant d'adresses IP sources uniques par minute et effectue des mises AWS WAF à jour pour bloquer les analyses ultérieures à partir 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, sont le nombre maximal de ressources ou d'opérations de service pour vous Compte AWS.

Quotas pour AWS les services 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, reportez-vous à la section Quotas AWS de service. Pour voir les quotas de service pour tous les AWS services de la documentation sans changer de page, consultez PDF plutôt les informations sur la page Points de terminaison et quotas du service.

AWS WAF quotas

AWS WAF peut bloquer un maximum de 10 000 plages d'adresses IP dans la notation Classless Inter-Domain Routing (CIDR) par condition de correspondance IP. Chaque liste créée par cette solution est soumise à ce quota. Pour plus d'informations, reportez-vous à la section AWS WAF Quotas. 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 pourIPv6.

AWS WAF autorise un maximum d'une demande par seconde, par compte, par Région AWS API appel à une personne `Create` ou par `Update` action. `Put` Si vous passez ces API appels en dehors de la solution, il se peut que vous rencontriez un API problème de régulation. Pour éviter ce problème, nous vous recommandons d'éviter d'exécuter d'autres applications effectuant ces API appels 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.

AWS WAF règles

Le Web généré par ACL cette solution est conçu pour offrir une protection complète aux applications Web. La solution fournit un ensemble AWS Managed Rules de règles personnalisées que vous pouvez ajouter au WebACL. 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.

Enregistrement ACL du trafic Web

Si vous créez la pile Région AWS ailleurs que dans 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 AWS WAF des journaux sur un site Web ACL qui fonctionne dans tous les emplacements AWS périphériques, 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 ACL du trafic Web, consultez le guide du AWS WAF développeur.

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 savoir AWS WAF quoi 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`— Traitez la requête Web comme correspondant à l'énoncé de règle. AWS WAF applique l'action de règle à la demande sans l'évaluer par rapport aux critères d'inspection de la règle. 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 du WebACL, 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 AWS WAF quotas par compte et par région.

Déployez la solution

Cette solution utilise des AWS CloudFormation modèles et des piles pour automatiser son déploiement. Les CloudFormation modèles spécifient les AWS ressources 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
- Configurez un ALB

Étape 1. Lancez la pile

- Lancez le CloudFormation modèle dans 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 le Web ACL à votre application Web

- Associez votre ou ALB vos distributions CloudFront Web au Web généré par ACL 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 et envoyez les fichiers journaux au compartiment Amazon S3 approprié. ALB 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 Logs (`AWS Logs/`préfixe de journal par défaut). AWS Consultez le paramètre Application Access Log Bucket Prefix à l'étape 1. Lancez la pile pour plus d'informations.

AWS CloudFormation modèles

Cette solution inclut un AWS CloudFormation modèle 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 un AWS WAF site Web ACL avec des règles préconfigurées. Vous pouvez personnaliser le modèle en fonction de vos besoins.

ACLStack Web

aws-waf-security-automations-webacl.template — Ce modèle imbriqué fournit des AWS WAF ressources, notamment un site WebACL, 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 relatives à Athena et Firehose. AWS Glue Il est créé lorsque vous choisissez l'analyseur de journaux Athena de Scanner & Probe ou l'analyseur de journaux Flood HTTPLambda ou Athena.

Prérequis

Cette solution est conçue pour fonctionner avec des applications Web déployées avec CloudFront ou unALB. 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).

Configurez un ALB

Pour configurer et distribuer le trafic entrant ALB 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 AWS CloudFormation modèle automatique déploie la solution sur le AWS Cloud.

1. Connectez-vous au AWS Management Consoleet sélectionnez Launch Solution 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 sous une autre forme 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 Régions AWS que de manière spécifique. Par conséquent, vous devez lancer cette solution Région AWS là où ces services sont disponibles. Pour plus d'informations, reportez-vous à Supporté Régions AWS.

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

Paramètre	Par défaut	Description
Nom de la pile	*`<requires input>`*	Le nom de la pile ne peut pas contenir d'espaces. Ce nom doit être unique au sein de votre Compte AWS entreprise et il s'agit du nom du site Web ACL créé par le modèle.
Type de ressource		
Point de terminaison	`CloudFront`	Choisissez le type de ressource utilisé.

Paramètre	Par défaut	Description
		Note Si vous `CloudFront` le souhaitez comme point de terminaison, vous devez lancer la solution pour créer WAF des ressources dans la région USA Est (Virginie du Nord) (`us-east-1`).
AWS Groupes de règles de réputation IP gérés		

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 sur le WebACL. 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 nombre requis WCU est de 25. Votre compte doit disposer d'une WCU capacité suffisante pour éviter l'échec du déploiement de Web ACL Stack en cas de dépasseme nt de la limite de capacité. Pour plus d'informations, consultez la liste des groupes de AWS Managed Rules règles.

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 sur le WebACL. 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 proxysVPNs, de nœuds Tor et de fournisseurs d'hébergement. Ce groupe de règles est utile si vous souhaitez filtrer les utilisate urs qui tentent de masquer leur identité auprès de votre application. Le blocage des adresses IP liées à ces services peut contribuer à limiter les robots et le non-respect des restrictions géographiques. Le nombre requis WCU est de 50. Votre compte doit disposer d'une WCU capacité suffisante pour éviter l'échec du déploiement de Web ACL Stack en cas de dépasseme nt de la limite de capacité.

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

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 au WebACL. 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 AWS WAF d'utilisation. Le nombre requis WCU est de 700. Votre compte doit disposer d'une WCU capacité suffisante pour éviter l'échec du déploiement de Web ACL Stack en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes de AWS Managed Rules règles.

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 au WebACL. 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 nombre requis WCU est de 100. Votre compte doit disposer d'une WCU capacité suffisante pour éviter l'échec du déploiement de Web ACL Stack en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes de AWS Managed Rules règles.

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 pour les entrées défectueuses connues sur le WebACL. 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 nombre requis WCU est de 100. Votre compte doit disposer d'une WCU capacité suffisante pour éviter l'échec du déploiement de Web ACL Stack en cas de dépasseme nt de la limite de capacité. Pour plus d'informations, consultez la liste des groupes de AWS Managed Rules règles.
AWS Groupe de règles spécifiques à un cas d'utilisation géré		

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés par la SQL base de données	no	Choisissez `yes` d'activer le composant conçu pour ajouter un groupe de règles géré par SQL base de données au WebACL. Ce groupe de règles bloque les modèles de demandes associés à l'exploitation de SQL bases de données, tels que les attaques SQL par injection. Cela peut aider à empêcher l'injecti on à distance de requêtes non autorisées. Évaluez ce groupe de règles à utiliser si votre application s'interfa ce avec une SQL base de données. L'utilisation de la règle personnalisée SQL d'injection est facultative si le groupe de SQL règles AWS géré est déjà activé. Le nombre requis WCU est de 200. Votre compte doit disposer d'une WCU capacité suffisante pour éviter l'échec du déploiement de Web ACL Stack en cas de dépasseme nt de la limite de capacité. Pour plus d'informations, consultez la liste des groupes

Paramètre	Par défaut	Description
		de AWS Managed Rules règles.

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 au WebACL. 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 POSIX d'exploitation. Le nombre requis WCU est de 200. Votre compte doit disposer d'une WCU capacité suffisante pour éviter l'échec du déploiement de Web ACL Stack en cas de dépassement de la limite de capacité.

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

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérés par le système d'POSIXex ploitation	no	Choisissez `yes` d'activer le composant conçu pour ajouter la protection des groupes de règles gérés par un ensemble de règles de base au WebACL. Ce groupe de règles bloque les modèles de demandes associés à l'exploitation de vulnérabilités spécifiques aux systèmes POSIX d'POSIXex ploitation similaires, y compris LFI les attaques. 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 POSIX d'exploitation POSIX ou similaire. Le nombre requis WCU est de 100. Votre compte doit disposer d'une WCU capacité suffisante pour éviter l'échec du déploiement de Web ACL Stack en cas de dépasseme nt de la limite de capacité. Pour plus d'informations, consultez la liste des groupes

Paramètre	Par défaut	Description
		de AWS Managed Rules règles.

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 au WebACL. 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 nombre requis WCU est de 200. Votre compte doit disposer d'une WCU capacité suffisante pour éviter l'échec du déploiement de Web ACL Stack en cas de dépassement de la limite de capacité. Pour plus d'informations, consultez la liste des groupes

Paramètre	Par défaut	Description
		de AWS Managed Rules règles.

Paramètre	Par défaut	Description
Activer la protection des groupes de règles gérée par les PHP applications	no	Choisissez `yes` d'activer le composant conçu pour ajouter un groupe de règles géré par l'PHPapplication au WebACL. Ce groupe de règles bloque les modèles de demandes associés à l'exploitation de vulnérabilités spécifiques à l'utilisation du langage de PHP programmation, notamment l'injection de PHP fonctions non sécurisées. Cela peut aider à 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 s'PHPil est installé sur un serveur avec lequel votre application s'interface. Le nombre requis WCU est de 100. Votre compte doit disposer d'une WCU capacité suffisante pour éviter l'échec du déploiement de Web ACL Stack en cas de dépasseme nt de la limite de capacité. Pour plus d'informations, consultez la liste des groupes

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

Paramètre	Par défaut	Description
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	*<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 votre ou ALB vos CloudFront distributions. Si vous utilisez un compartiment Amazon S3 existant, il doit se trouver à l' Région AWS endroit même où vous déployez le CloudFormation modèle. Vous devez utiliser un compartiment différent pour chaque déploiement de solution. Pour désactiver cette protection, ignorez ce paramètre. **Note** Activez la journalisation des accès CloudFront Web pour vos distributions Web afin d'ALBenvoyer des fichiers journaux vers ce compartiment Amazon S3. Enregistrez les journaux dans

Paramètre	Par défaut	Description
		le même préfixe défini dans la pile (préfixe `AWS Logs/` par défaut). Consultez le paramètre Application Access Log Bucket Prefix pour plus d'informations.

Paramètre	Par défaut	Description
Préfixe du compartiment du journal d'accès aux applications	`AWS Logs/`	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 `AWS Logs/` à votre préfixe tel que. `yourprefix/AWSLogs/` Utiliser `AWS Logs/` (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 par inondation. 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
Seuil de demande par défaut	`100`	Si vous avez choisi `yes` le paramètre Activer la protection contre les HTTP inondations, entrez le nombre maximum 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 contre les HTTP inondations, la valeur minimale acceptable est`100`. Si vous avez choisi `yes - AWS Lambda log parser` ou `yes – Amazon Athena log parser` pour le paramètre Activer la protection contre les HTTP inondations, 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 contre les HTTP inondations, vous pouvez saisir un seuil par pays en suivant ce JSON format`{"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. **Note** Si vous définisse z 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 Flood HTTP Athena Query.

Paramètre	Par défaut	Description
		Si vous avez choisi de désactiver cette protection, ignorez ce paramètre.
Regrouper par requêtes dans HTTP Flood Athena Query	`None`	Si vous avez choisi `yes - Amazon Athena log parser` le paramètre Activer la protection contre les HTTP 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`URI`. Si vous avez choisi de désactiver cette protection, ignorez ce paramètre.

Paramètre	Par défaut	Description
WAFPériode de blocage	`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.
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.
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.
ARNd'un IAM rôle disposant d'un accès en écriture aux CloudWatch journaux de votre compte	<optional input>	Indiquez un IAM rôle facultatif disposant ARN d'un accès en écriture aux CloudWatch journaux de votre compte. olpPar exemple : `ARN: arn:aws:iam::account_id:role/myrolename` . Consultez Configuration de la CloudWatch journalisation pour une REST API API passerelle intégrée pour obtenir des instructions sur la création du rôle. Si vous laissez ce paramètre vide (par défaut), la solution vous crée un nouveau rôle.

Paramètre	Par défaut	Description
Seuil de demande par défaut	100	Si vous avez choisi `yes` le paramètre Activer la protection contre les HTTP inondations, entrez le nombre maximum 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 contre les HTTP inondations, la valeur minimale acceptable est 100. Si vous avez choisi `yes - AWS Lambda log parser` ou `yes – Amazon Athena log parser` pour le paramètre Activer la protection contre les HTTP inondations, il peut s'agir de n'importe quelle valeur. Pour désactiver cette protection, ignorez ce paramètre.
Règle personnalisée — Listes de réputation IP de tiers		

Paramètre	Par défaut	Description
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 SQL injections	`yes`	Choisissez `yes` d'activer le composant conçu pour bloquer les attaques SQL d'injection courantes. Envisagez de l'activer si vous n'utilisez pas un ensemble de règles de base de SQL données AWS AWS géré ou un groupe de règles de base de données géré. Vous pouvez choisir l'une des options `yes` (continuer) ou`yes - NO_MATCH`) selon laquelle vous souhaitez traiter les demandes surdimens ionnées supérieures AWS WAF à 8 Ko (8192 octets). `yes - MATCH` Par défaut, `yes` 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 requêtes Web surdimensionnés. Choisissez no de désactiver cette fonctionnalité.

Paramètre	Par défaut	Description
		Note La CloudFormation pile ajoute l'option de gestion des surdimensionnements sélectionnée à la règle de protection par SQL injection 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 SQL injections	`LOW`	Choisissez le niveau de sensibilité que vous AWS WAF souhaitez utiliser pour détecter les attaques SQL par injection. `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 SQL par injection ou qui tolèrent peu les faux positifs. Pour plus d'informations, reportez-vous à la section AWS WAF Ajouts des niveaux de sensibilité pour les instructions et les SensitivityLevelpropriétés des règles d'SQLinjection dans le Guide de AWS CloudFormation l'utilisateur. Si vous choisissez de désactiver la protection contre les SQL injections, ignorez ce paramètre.

Paramètre	Par défaut	Description
		Note La CloudFormation pile ajoute le niveau de sensibilité sélectionné à la règle de protection par SQL injection 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 XSS attaques courantes. Envisagez de l'activer si vous n'utilise z pas un ensemble de règles de base AWS géré. Vous pouvez également sélectionner l'une des options (`yes`(continuer) ou`yes - NO_MATCH`) selon laquelle vous souhaitez traiter les demandes surdimensionnées supérieures AWS WAF 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 désactiver cette fonctionnalité. **Note** La CloudFormation pile ajoute l'option de gestion des

Paramètre	Par défaut	Description
		surdimensionnements sélectionnée à la règle de script intersite 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.
Paramètres de conservation des adresses IP autorisés et refusés		

Paramètre	Par défaut	Description
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 IAM ressources et toutes les fonctionnalités supplémentaires requises.
9. Choisissez Submit pour déployer la pile.

   Consultez l'état de la pile dans la AWS CloudFormation console dans la colonne État. Vous devriez recevoir le statut CREATE _ COMPLETE dans 15 minutes environ.

   > **Note**
   >
   > Outre les fonctions, et `Log ParserIP Lists Parser`, cette solution inclut `Access Handler` AWS Lambda les fonctions `helper` et `custom-resource` Lambda, qui s'exécutent uniquement lors de la configuration initiale ou lorsque des ressources sont mises à jour ou supprimées.
   > Lorsque vous utilisez cette solution, toutes les fonctions s'affichent dans la AWS Lambda console, 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, qui est le point de terminaison du pot de miel API Gateway. N'oubliez pas cette valeur car vous l'utiliserez dans Intégrer le lien Honeypot dans votre application Web.

Étape 2. Associez le Web ACL à votre application Web

Mettez à jour vos CloudFront distributions pour les activer AWS WAF et les enregistrer en utilisant les ressources que vous avez générées à l'étape 1. ALB Lancez la pile.

1. Connectez-vous à la console AWS WAF.
2. Choisissez le site Web ACL que vous souhaitez utiliser.
3. Dans l'onglet AWS Ressources associées, choisissez Ajouter AWS des ressources.
4. Sous Type de ressource, choisissez la CloudFront distribution ouALB.

5. Sélectionnez une ressource dans la liste, puis choisissez Ajouter pour enregistrer vos modifications.

Étape 3. Configuration de la journalisation des accès web

Configurez CloudFront ou envoyez ALB 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 au Web à partir 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 le AWS WAF Web ACL, choisissez la ACL solution 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 énumère les compartiments associés au compartiment actuel. Compte AWS 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`AWS Logs/`).
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 (AmazonEC2).
2. Dans le volet de navigation, choisissez Load Balancers.

3. Sélectionnez celles de votre application WebALB.
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`AWS Logs/`).
8. Choisissez Save (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.

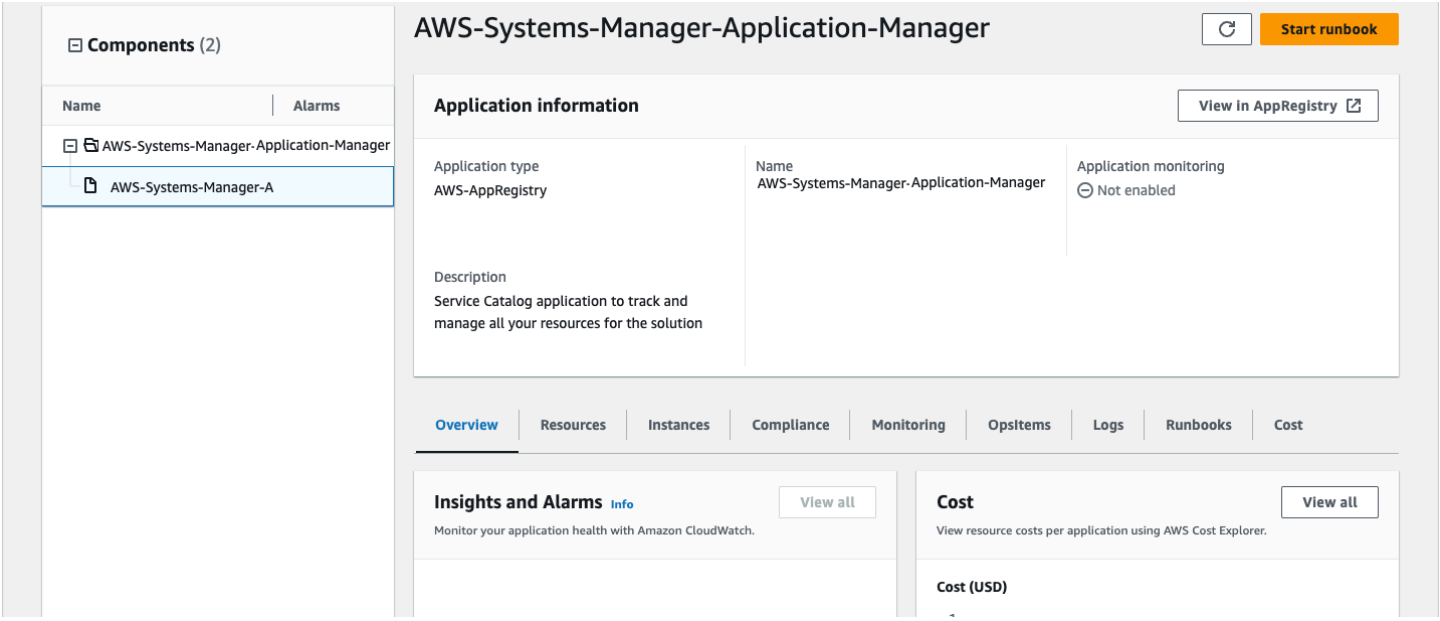
Surveillez la solution avec AppRegistry

La solution inclut une AppRegistry ressource Service Catalog pour enregistrer le CloudFormation modèle et les ressources sous-jacentes en tant qu'application dans Service Catalog AppRegistry et AWS Systems Manager Application Manager.

AWS Systems Manager Application Manager vous donne une vue d'ensemble de cette solution et de ses ressources au niveau de l'application, afin que vous puissiez :

- Surveillez ses ressources, les coûts des ressources déployées sur plusieurs piles et Comptes AWS les journaux associés à cette solution à partir d'un emplacement central.
- Affichez les données d'exploitation des ressources de cette solution dans le contexte d'une application. Par exemple, l'état du déploiement, les CloudWatch alarmes, les configurations des ressources et les problèmes opérationnels.

La figure suivante illustre un exemple de vue d'application pour la pile de solutions dans Application Manager.



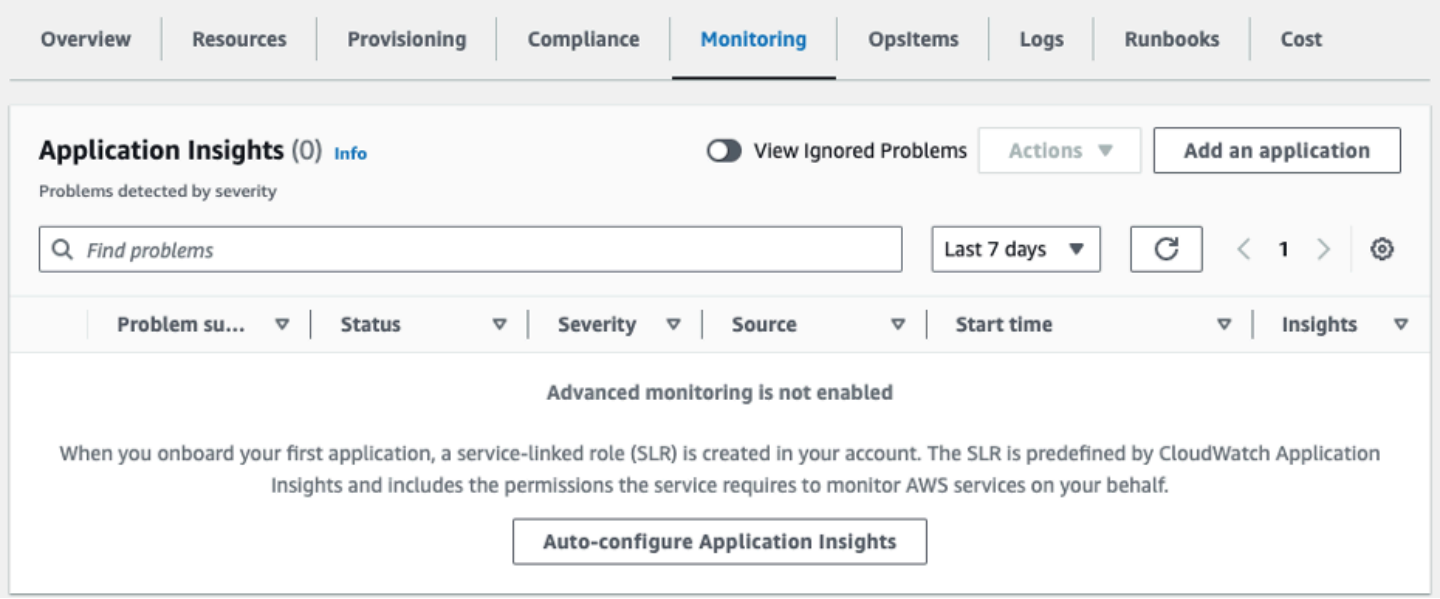
Pile de solutions dans le gestionnaire d'applications

Activer CloudWatch Application Insights

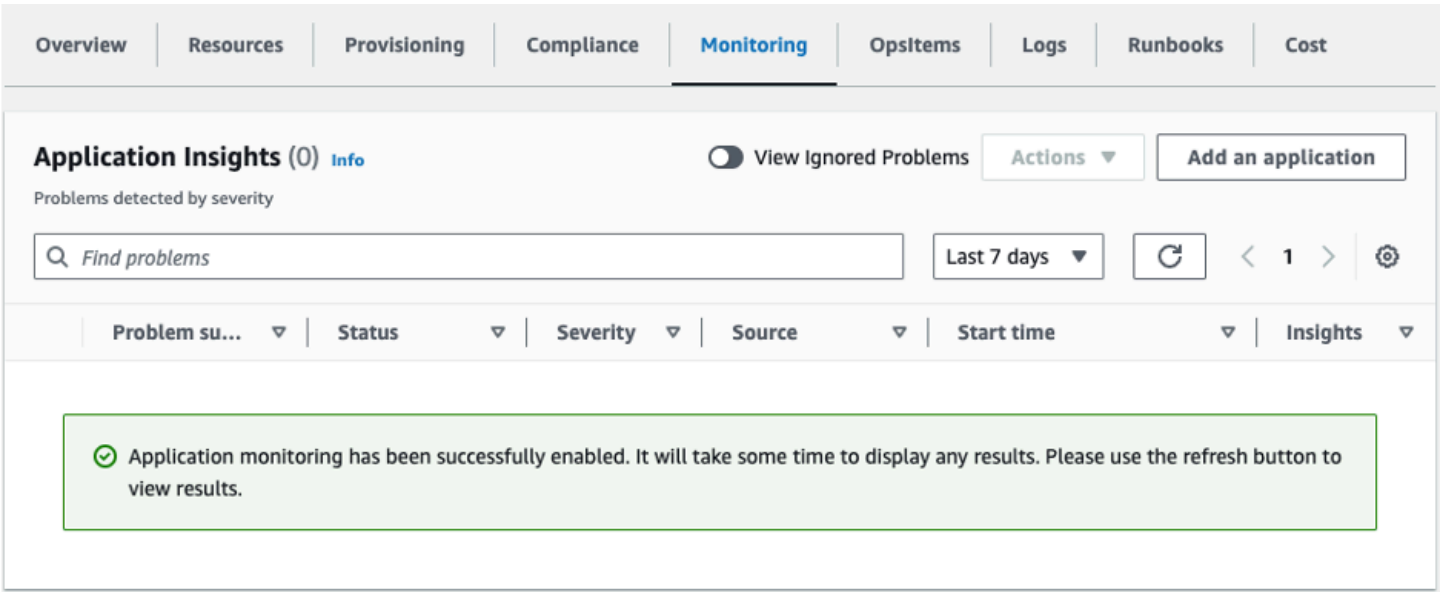
1. Connectez-vous à la console Systems Manager.

2. Dans le volet de navigation, choisissez Application Manager.
3. Dans Applications, recherchez le nom de l'application pour cette solution et sélectionnez-la.

   Le nom de l'application indiquera App Registry dans la colonne Source de l'application et comportera une combinaison du nom de la solution, de la région, de l'ID de compte ou du nom de la pile.
4. Dans l'arborescence des composants, choisissez la pile d'applications que vous souhaitez activer.
5. Dans l'onglet Surveillance, dans Application Insights, sélectionnez Configurer automatiquement Application Insights.



La surveillance de vos applications est désormais activée et la boîte de statut suivante apparaît :

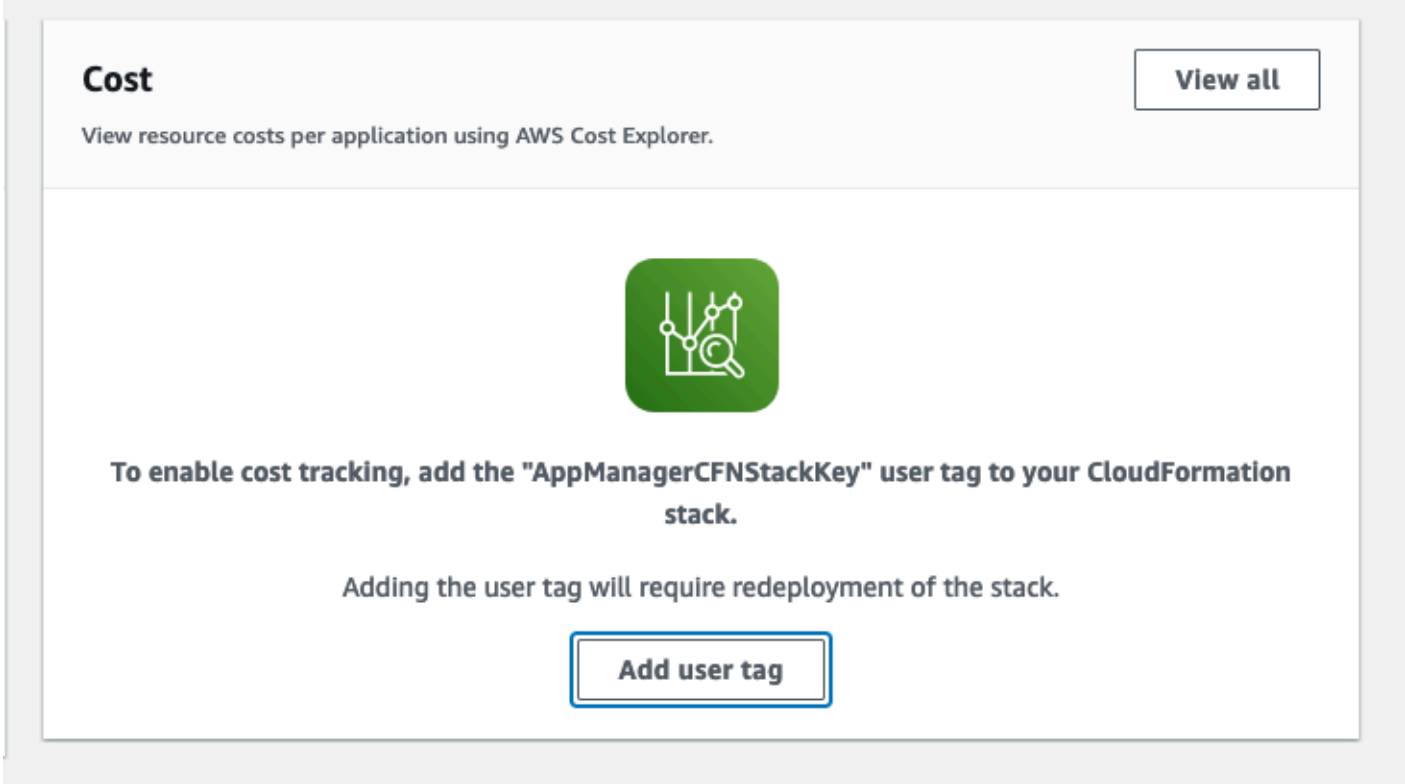


Confirmez les étiquettes de coût associées à la solution

Après avoir activé les balises de répartition des coûts associées à la solution, vous devez confirmer les balises de répartition des coûts pour connaître les coûts de cette solution. Pour confirmer les balises de répartition des coûts :

1. Connectez-vous à la console Systems Manager.
2. Dans le volet de navigation, choisissez Application Manager.
3. Dans Applications, choisissez le nom de l'application pour cette solution, puis sélectionnez-la.

   Le nom de l'application indiquera App Registry dans la colonne Source de l'application et comportera une combinaison du nom de la solution, de la région, de l'ID de compte ou du nom de la pile.
4. Dans l'onglet Aperçu, dans Coût, sélectionnez Ajouter un tag utilisateur.



5. Sur la page Ajouter un tag utilisateur, entrez`confirm`, puis sélectionnez Ajouter un tag utilisateur.

Le processus d'activation peut prendre jusqu'à 24 heures et les données du tag peuvent apparaître.

Activez les balises de répartition des coûts associées à la solution

Après avoir activé Cost Explorer, vous devez activer les balises de répartition des coûts associées à cette solution pour connaître les coûts de cette solution. Les balises de répartition des coûts ne peuvent être activées qu'à partir du compte de gestion de l'organisation. Pour activer les balises de répartition des coûts :

1. Connectez-vous à la console AWS Billing and Cost Management and Cost Management.
2. Dans le volet de navigation, sélectionnez Balises de répartition des coûts.
3. Sur la page Balises de répartition des coûts, filtrez le AppManager CFNStackKey tag, puis sélectionnez-le parmi les résultats affichés.
4. Choisissez Activer.

AWS Cost Explorer

Vous pouvez consulter l'aperçu des coûts associés à l'application et aux composants de l'application dans la console Application Manager grâce à l'intégration avec AWS Cost Explorer, qui doit d'abord être activée. Cost Explorer vous aide à gérer les coûts en fournissant une vue des coûts et de l'utilisation de vos AWS ressources au fil du temps. Pour activer Cost Explorer pour la solution, procédez comme suit :

1. Connectez-vous à la console de gestion des AWS coûts.
2. Dans le volet de navigation, sélectionnez Cost Explorer pour visualiser les coûts et l'utilisation de la solution au fil du temps.

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 console AWS CloudFormation.
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. Cliquez sur Amazon S3URL.
   b. Copiez le lien du `aws-waf-security-automations.template` AWS CloudFormation.
   c. Collez le lien dans le URL champ Amazon S3.
   d. Vérifiez que le modèle correct URL apparaît dans la zone de URL texte 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 obtenir des informations détaillées sur les paramètres.
8. Choisissez 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 IAM des ressources.
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 AWS CloudFormation console dans la colonne État. 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.

WAFV2mise à niveau

À partir de la version 3.0, cette solution prend en charge la AWS WAF V2. Nous avons remplacé tous les API appels AWS WAF classiques par des APIappels AWS WAF V2. 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 AWS WAF règles avec des configurations par défaut dans votre Compte AWS CloudFormation stack. 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.

> **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 update-ip-setCLIcommandes get-ip-setet. 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 console AWS CloudFormation.

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 AWS ressources 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 AWAWAFAPIquotas, 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.

Cependant, les robots et les scrapeurs de contenu, tels que les malwares qui détectent les failles de sécurité et suppriment les adresses e-mail, peuvent tenter d'accéder au point de terminaison du piège. Dans ce scénario, la fonction `Access Handler` Lambda inspecte la demande pour en extraire l'origine, puis met à jour la AWS WAF règle associée pour bloquer les demandes suivantes provenant de cette adresse IP.

Utilisez l'une des procédures suivantes pour intégrer le lien honeypot pour les demandes provenant d'une CloudFront distribution ou d'un. ALB

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 console AWS CloudFormation.
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 le point de terminaisonURL. Il contient deux éléments dont vous avez besoin pour effectuer cette procédure :
   - Le nom d'hôte du point de terminaison (par exemple,`xxxxxxxxxx.execute-api.region.amazonaws.com`)
   - La demande URI (`/ProdStage`)
5. Connectez-vous à la CloudFront console Amazon.
6. Choisissez la distribution que vous souhaitez utiliser.
7. Choisissez Paramètres de distribution.
8. Sous l'onglet Origines, choisissez Créer une origine.
9. Dans le champ Nom de domaine d'origine, collez le composant de nom d'hôte du point de terminaison URL que vous avez copié à l'étape 2. Associez le Web ACL à votre application Web.
10. Dans Origin Path, collez la demande URL que vous avez également copiée à l'étape 2. Associez le Web ACL à votre application Web.
11. Acceptez les valeurs par défaut pour les autres champs.
12. Sélectionnez Create (Créer).
13. Sous l'onglet Comportements, choisissez Comportement de cache.
14. Créez un nouveau comportement de cache et pointez-le vers la nouvelle origine. Vous pouvez utiliser un domaine personnalisé, tel qu'un faux nom de produit similaire à d'autres contenus de votre application Web.
15. 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>
```

> **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.

16 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>
```

Intégrer le point de terminaison Honeypot en tant que lien externe

Utilisez cette procédure pour les applications Web déployées avec unALB.

1. Connectez-vous à la console AWS CloudFormation.
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 le point de terminaisonURL.
5. Intégrez ce lien de point de terminaison dans votre contenu Web. Utilisez le fichier complet URL que vous avez copié à l'étape 2. Associez le Web ACL à votre application Web. Cachez ce lien à vos utilisateurs humains. À titre d'exemple, consultez l'exemple de code suivant :

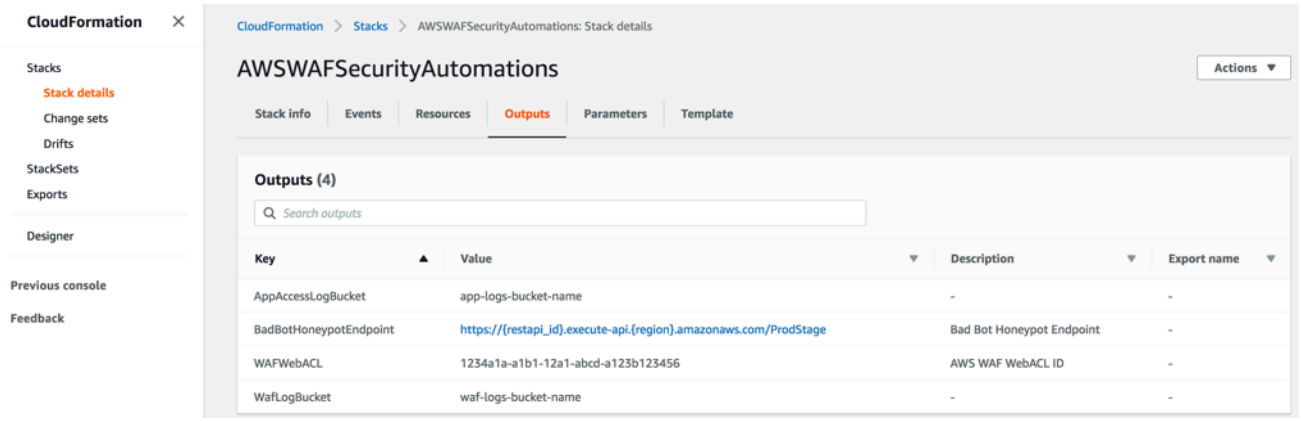
```
<a href="<BadBotHoneypotEndpoint value>" rel="nofollow" style="display: none" aria-
hidden="true"><honeypot link></a>
```

> **Note**
>
> Cette procédure permet de demander `rel=nofollow` aux robots de ne pas accéder au pot de mielURL. 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 d'analyseur de journal Lambda JSON

Utiliser le JSON fichier d'analyse du journal Lambda pour la protection contre les inondations HTTP

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 AWS WAF journaux. Pour trouver le nom du compartiment, reportez-vous à la WafLogBucketvariable dans la CloudFormation sortie. La figure suivante montre un exemple.



Sorties empilées

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 AWS WAF des nouveaux fichiers journaux. Voici un exemple de fichier de configuration :

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

HTTPfichier de configuration Flood

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.
- URIlist — Utilisez-le pour définir un seuil de demande personnalisé et une période de blocage pour des informations spécifiques. URLs Par défaut, cette liste est vide.

Lorsque WAF les journaux 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'WAFadresse IP définie pour HTTPFlood 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 a été dépassée conformément au fichier de configuration.

Utiliser le JSON fichier d'analyse du journal Lambda pour la protection du scanner et de la sonde

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 AWS WAF des nouveaux fichiers journaux. Voici un exemple de fichier de configuration :

Fichier de configuration des scanners et des sondes

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 : renvoie le code d'état considéré comme une erreur. Par défaut, la liste considère les codes HTTP d'état suivants comme des erreurs : `400 (Bad Request)401 (Unauthorized)`,`403 (Forbidden)`,`404 (Not Found)`, et`405 (Method Not Allowed)`.

- URIlist — Utilisez-le pour définir un seuil de demande personnalisé et une période de blocage pour des informations spécifiquesURLs. 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'WAFadresse IP 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.

Utilisez le pays et l'URIanalyseur de HTTP log Athena en cas d'inondation

Vous pouvez les regrouper IPs par pays et URI dans la requête Athena pour détecter et bloquer les HTTP inondations dont le schéma est imprévisibleURI. 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 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 CloudFront or ALB (`ScannersProbesLogParser`) ou AWS WAF logs (`HTTPFloodLogParser`), analyse la sortie et met à jour en conséquence. AWS WAF

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 analysées par une requête en modifiant la valeur du paramètre du modèle WAFBlock 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. AWS AWS Glue Data Catalog Cette solution crée le catalogue de données des journaux d'accès 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 la dernière version AWSAWS Glue Data Catalog step-by-step.

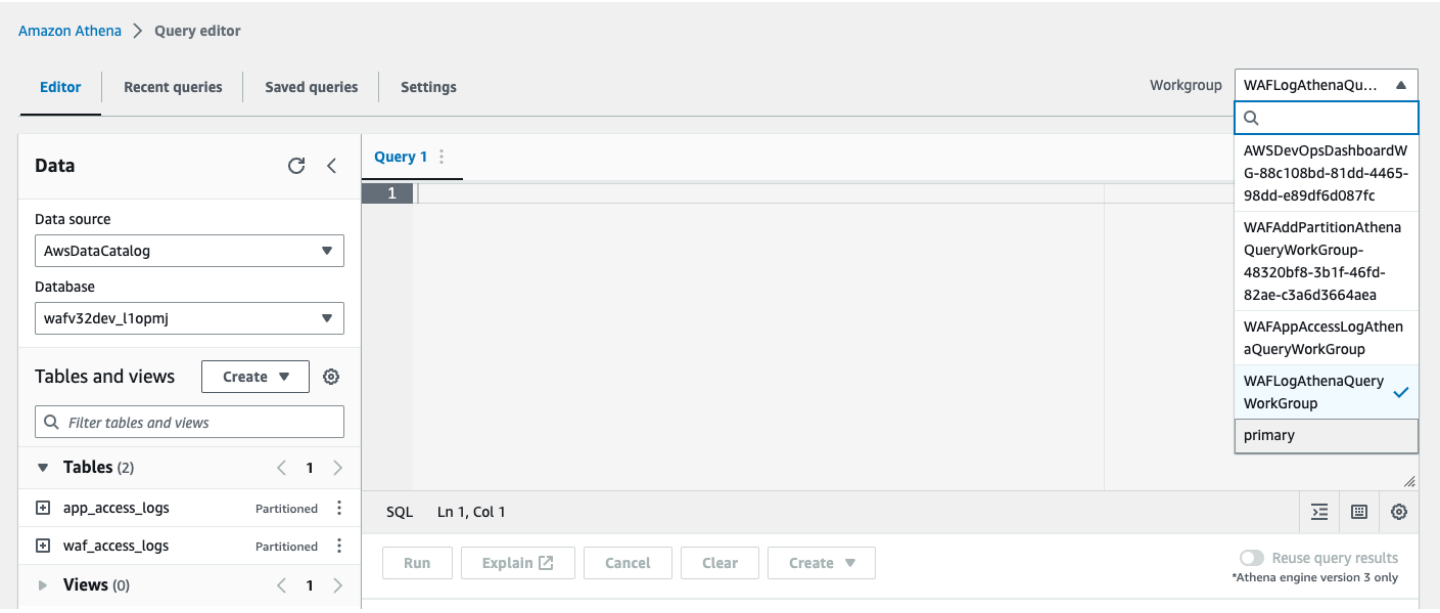
Pour consulter ces requêtes, procédez comme suit :

Afficher les requêtes du WAF journal

1. Connectez-vous à la console Amazon Athena.
2. Choisissez Lancer l'éditeur de requêtes.
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 Activer la protection contre les HTTP inondations.

5. Choisissez Switch pour changer de groupe de travail.



6. Sélectionnez l'onglet Historique.
7. 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.

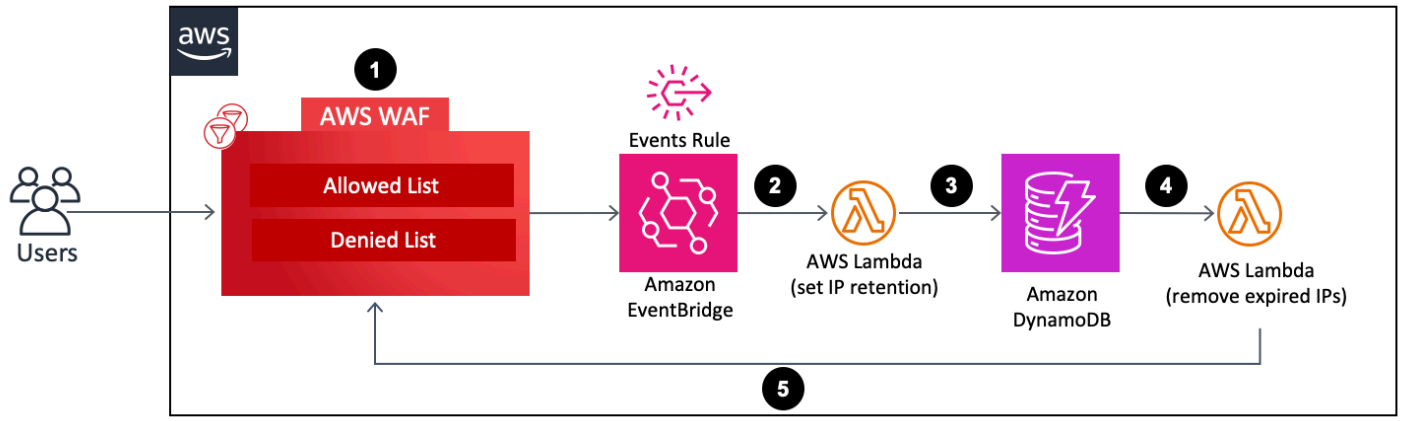
> **Note**
>
> Ce groupe de travail n'existe que si vous avez sélectionné le paramètre `Yes - Amazon Athena log parser` de modèle Activate HTTP Flood Protection et/ou Activate Scanner & Probe Protection.

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.

Configurer la rétention des adresses IP sur les ensembles d' AWS WAF adresses IP autorisées et refusées

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

Fonctionnement



Conservation des adresses IP sur les ensembles d'WAFadresses IP autorisés et refusés

1. Lorsqu'un utilisateur met à jour (ajoute ou supprime une adresse IP) l'ensemble d'adresses WAF IP autorisées ou refusées, cette action appelle un AWS WAF `UpdateIPSet` API appel 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'TTLattribut est`ExpirationTime`.
4. Lorsqu'un élément atteint son délai d'expiration, TTL il 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 AWS WAF API appel pour supprimer les adresses IP expirées incluses dans l'élément de l'ensemble d'adresses IP cible. AWS WAF

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 tout 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 AWS WAF IP. 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' AWS WAF adresse IP définie 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' AWS WAF adresse IP définie 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 de l'ensemble d'adresses IP les adresses IP incluses dans la liste d'adresses IP de l'élément. WAF

> **Note**
>
> En fonction de l'heure à laquelle DynamoDB supprime un élément expiréTTL, l'opération de suppression effective d'une adresse IP expirée de l'ensemble d'adresses IP peut varier AWS WAF . La suppression de TTL DynamoDB dépend principalement de la taille et du niveau d'activité d'une table. Attendez-vous à un retard dans l'opération de AWS WAF suppression en raison du retard potentiel de l'opération de suppression DynamoDB. En général, la solution supprime les adresses IP expirées de l'adresse AWS WAF IP définie peu de temps après la suppression de DynamoDBTTL. 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 CloudWatchTableaux 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.

Le tableau de bord affiche les statistiques suivantes :

- Demandes autorisées ou bloquées — Indique si vous recevez une augmentation du nombre d'accès autorisés (deux fois le pic d'accès normal) ou d'accès bloqué (toute période identifiant plus de 1 000 demandes bloquées). CloudWatch envoie une alerte à une chaîne Slack. Vous pouvez utiliser cette métrique pour suivre DDoS les attaques 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 le moment où une DDoS attaque cible un service qui ne reçoit normalement pas beaucoup d'accès pour épuiser les ressources (par exemple, un composant du moteur de recherche envoie MBs des informations pour un ensemble de paramètres de demande spécifique).

- ELBIncidence et longueur de la file d'attente : permet de vérifier si une DDoS attaque endommage l'infrastructure et si l'attaquant contourne CloudFront la AWS WAF couche et attaque directement les ressources non protégées.
- ELBNombre de demandes : 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.
- ELBHealthy Host — Vous pouvez l'utiliser comme une autre mesure de vérification de l'état du système.
- ASGCPUUtilisation — Permet d'identifier si l'attaquant contourne CloudFront Elastic Load Balancing. AWS WAF Vous pouvez également utiliser cette métrique pour identifier les dégâts d'une attaque.

Gérez les XSS faux positifs

Cette solution configure une AWS WAF règle qui inspecte les éléments fréquemment explorés des demandes entrantes afin d'identifier et de bloquer XSS les attaques. Ce modèle de détection est moins efficace si votre charge de travail permet à des utilisateurs légitimes de composer et de soumettreHTML, 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 XSS règle par défaut pour les URL modèles spécifiques qui acceptent la saisie de texte enrichi, et de mettre en œuvre des mécanismes alternatifs pour protéger les personnes excluesURLs.

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

Procédez comme suit pour mettre à jour la XSS règle afin d'exclure URLs cette acceptation HTML en tant qu'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 URI et répertorier les valeurs que vous souhaitez accepter par rapport à la XSS règle.

4. Modifiez la XSSrègle 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
   - XSSListe d'autorisations

Résolution des problèmes

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

Contacter Support

Si vous bénéficiez AWSdu Support aux développeurs, du Support aux AWS AWS entreprises ou du Support aux entreprises, vous pouvez utiliser le Centre de support pour obtenir l'assistance d'experts sur 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. Pour Service, sélectionnez WAFou AWS WAF.
3. Dans Catégorie, sélectionnez Automatisations WAFde sécurité ou 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. Dans le champ Description, décrivez le problème en détail.
3. Choisissez Joindre des fichiers.
4. Joignez les informations Support nécessaires au traitement de la demande.

Aidez-nous à résoudre votre cas plus rapidement

1. Entrez les informations demandées.
2. Choisissez Next step: Solve now or contact us (Étape suivante : résolvez maintenant ou contactez-nous).

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 GitHubréférentiel pour télécharger les modèles et les scripts de cette solution et pour partager vos personnalisations avec d'autres utilisateurs.

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 AWS lors du déploiement initial du CloudFormation modèle :

- ID de solution : identifiant de AWS solution
- 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 l'ensemble d'adresses IP Scanner & Probe et dans l'adresse IP HTTPFlood configurée 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 du gestionnaire d'accès :
  - Le nombre d'adresses IP dans l'ensemble d'adresses IP de Bad Bot
  - 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 détient les données recueillies dans le cadre de cette enquête. La collecte de données est soumise à la AWS Politique de confidentialité. Pour désactiver cette fonctionnalité, suivez les étapes ci-dessous avant de lancer le AWS CloudFormation modèle.

1. `aws-waf-security-automations.template`AWS CloudFormationTéléchargez-le 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 console AWS CloudFormation.
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 AWS blancs associés

- AWS Meilleures pratiques en matière de DDoS résilience

Articles AWS de blog sur la sécurité associés

- Comment empêcher les hotlinking en utilisant AWS WAF Amazon et Referer CloudFront Checking

Listes de réputation IP de tiers

- Site web de Spamhaus DROP List
- Liste 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

Révisions

Date	Modification
Septembre 2016	Première version
Janvier 2017	Clarification sur les limites d'adresses IP dans cette solution.
Mars 2017	Conseils supplémentaires sur la création d'un comportement de cache ; mis à jour URLs pour les articles du blog sur AWS la sécurité.
Juin 2017	ALBSupport supplémentaire et limites de produits mises à jour.
novembre 2017	Ajout de la prise en charge des règles basées sur les taux pour la protection contre les HTTP inondations ; liens supplémentaires pour le stockage des journaux d'accès aux ressources.
Janvier 2018	Contenu mis à jour sur la disponibilité régionale AWS WAF des équilibreurs de charge d'applica tion.
Décembre 2018	IPv6Support ajouté, CIDR gammes étendues et ajout d'un tableau de bord de surveillance.
Avril 2019	AWS WAF intégration des journaux, intégrati on d'Amazon Athena et ajout d'un analyseur de journaux configurable.
Décembre 2019	Ajout d'informations sur la prise en charge de la mise à jour de Node.js.
Février 2020	Corrections de bogues et mise à jour du RequestThreshold paramètre.

Date	Modification
Juin 2020	Ajout de l'optimisation des coûts d'Athena à l'aide du partitionnement ; mise à jour des README instructions ; correction d'un éventuel problème de DoS dans l'en-tête Bad Bots. X-Forward-For
juillet 2020	Mise à niveau du service AWS WAF Classic vers le service AWS WAF V2API.
Novembre 2020	Version 3.1.0 : clarification des règles de protection contre les HTTP inondations et de protection contre les scanners et les sondes pour des régions spécifiques ; remplacement du type de chemin S3 par un style hébergé virtuellement ; ajout d'une variable de partition à tous ARNs ; pour plus d'informations, reportez-vous au CHANGELOGfichier .md du référentiel. GitHub
septembre 2021	Version 3.2.0 : ajout de la prise en charge de la conservation des adresses IP sur les ensembles d'adresses IP autorisés et refusés ; corrections de bugs. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.
Août 2022	Version 3.2.1 : ajout de la prise en charge de la gestion des composants WAF surdimensionnés pour les composants de demande ; ajout de la prise en charge des niveaux de WAF sensibili té pour les instructions de règles SQL d'injecti on. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.

Date	Modification
Septembre 2022	Documentation mise à jour pour la personnal isation en dehors de la CloudFormation pile de la solution.
Décembre 2022	Version 3.2.2 : intégration ajoutée avec Service Catalog AppRegistry et AWS Systems Manager Application Manager. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.
Décembre 2022	Version 3.2.3 : Ajoutez une région comme préfixe au nom du groupe d'attributs de l'application pour éviter tout conflit avec le nom commençant par. AWS Pour plus d'informa tions, reportez-vous au fichier CHANGELOG .md du GitHub référentiel.
Février 2023	Version 3.2.4 : pytest mis à niveau et demandes d'atténuation. CVE Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.
Mars 2023	Documentation mise à jour pour la mise à niveau d'une solution de la version 3.0 ou 3.1 vers la version 3.2 ou ultérieure qui a autorisé ou refusé des adresses IP.
Avril 2023	Version 3.2.5 : impact atténué causé par les nouveaux paramètres par défaut pour la propriété des objets Amazon S3 (ACLsdésa ctivés) pour tous les nouveaux compartiments Amazon S3. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.

Date	Modification
Mai 2023	Version 4.0.0 : ajout de la prise en charge des nouveaux groupes de AWS Managed Rules règles et mise à jour des règles personnalisées. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.
Mai 2023	Version 4.0.1 : `.gitignore` fichier mis à jour pour résoudre le problème des fichiers manquants. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.
Septembre 2023	Version 4.0.2 : Code refactorisé pour améliorer la qualité. Vulnérabilité liée aux paquets de requêtes corrigés. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.
Octobre 2023	Version 4.0.3 : versions des packages mises à jour pour résoudre les failles de sécurité. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.
Novembre 2023	Mise à jour de la documentation : ajout AWS du support aux développeurs et fusion du AWS support de contact dans la section Dépannage.
Novembre 2023	Mise à jour de la documentation : ajout des balises de coût de confirmation associées à la solution dans la AppRegistry section Surveilla nce de la solution avec AWS Service Catalog.
Avril 2024	Mise à jour de la documentation : instructions clarifiées pour l'ajout d'un compartiment S3 à l'étape 3 du déploiement.

Date	Modification
Septembre 2024	Version 4.0.4 : versions des packages mises à jour pour résoudre les failles de sécurité. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.
Octobre 2024	Version 4.0.5 : Used Poetry pour la gestion des dépendances. L'enregistreur Python natif a été remplacé par l'enregistreur aws_lambda_powertools. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.
décembre 2024	Version 4.0.6 : mise à jour du lambda vers python 3.12. Pour plus d'informations, reportez-vous au fichier CHANGELOG.md du GitHub référentiel.

Avis

Ce guide de mise en œuvre est fourni à titre informatif uniquement. Il représente les offres de AWS produits et les pratiques actuelles 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 AWS produits ou services, 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 de ses filialesAWS, 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 AWS WAF solution Security Automations for 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.