Mettre en œuvre une stratégie de contrôle des bots sur AWS

AWS Conseils prescriptifs

AWS Conseils prescriptifs: Mettre en œuvre une stratégie de contrôle des bots sur AWS

Table of Contents

Mettre en œuvre une stratégie de contrôle des bots sur AWS

Amazon Web Services (contributeurs)

Février 2024 (historique du document)

Internet tel que nous le connaissons ne serait pas possible sans les robots. Les robots exécutent des tâches automatisées sur Internet et simulent l'activité ou l'interaction humaine. Ils permettent aux entreprises d'intégrer l'efficacité dans leurs processus et leurs tâches. Des robots utiles, tels que les robots d'exploration Web, indexent les informations sur Internet et nous aident à trouver rapidement les informations les plus pertinentes pour nos requêtes de recherche. Les bots sont un bon mécanisme pour améliorer les affaires et apporter de la valeur aux entreprises. Cependant, avec le temps, les acteurs malveillants ont commencé à utiliser des robots pour abuser des systèmes et applications existants de manière nouvelle et créative.

Les botnets sont le mécanisme le plus connu pour faire évoluer les bots et leur impact. Les botnets sont des réseaux de robots infectés par des malwares et placés sous le contrôle d'une seule entité, connue sous le nom de bot herder ou d'opérateur de bots. À partir d'un point central, l'opérateur peut commander à chaque ordinateur de son botnet d'exécuter simultanément une action coordonnée. C'est pourquoi les botnets sont également appelés systèmes command-and-control (C2).

L'échelle d'un botnet peut atteindre plusieurs millions de bots. Un botnet aide l'opérateur à effectuer des actions à grande échelle. Les botnets restant sous le contrôle d'un opérateur distant, les machines infectées peuvent recevoir des mises à jour et modifier leur comportement à la volée. Par conséquent, pour un gain financier significatif, les systèmes C2 peuvent louer l'accès à des segments de leur botnet sur le marché noir.

La prévalence des botnets n'a cessé de croître. Il est considéré par les experts comme l'outil préféré des mauvais acteurs. Mirai est l'un des plus grands botnets. Il est apparu en 2016, est toujours opérationnel et on estime qu'il a infecté jusqu'à 350 000 appareils de l'Internet des objets (IoT). Ce botnet a été adapté et utilisé pour de nombreux types d'activités, notamment les attaques par déni de service distribué (DDoS). Plus récemment, des acteurs malveillants ont tenté de masquer davantage leur activité et de générer leur trafic en obtenant des adresses IP grâce à l'utilisation de services de proxy résidentiels. Cela crée un peer-to-peer système légitime et interconnecté qui ajoute de la sophistication à l'activité et la rend plus difficile à détecter et à atténuer.

Ce document se concentre sur le paysage des bots, son effet sur vos applications, ainsi que sur les stratégies et les options d'atténuation disponibles. Ce guide prescriptif et ses meilleures pratiques

vous aident à comprendre et à atténuer les différents types d'attaques de robots. En outre, ce guide décrit les Services AWS fonctionnalités qui soutiennent une stratégie d'atténuation des bots et explique comment chacune d'entre elles peut vous aider à protéger vos applications. Il inclut également un aperçu de la surveillance des bots et des meilleures pratiques pour optimiser les coûts des solutions.

Comprendre les menaces et les opérations des robots

Selon Security Today, plus de 47 % de l'ensemble du trafic sur Internet est dû à des bots. Cela inclut la partie utile des robots, ceux qui s'identifient eux-mêmes et apportent de la valeur. Environ 30 % du trafic de bots est constitué de robots non identifiés qui mènent des activités malveillantes, telles que des attaques DDoS, le scalping de tickets, le scraping d'inventaire ou la thésaurisation. Security Magazine fait état d'une augmentation de 300 % du nombre d'événements DDoS volumétriques au cours du premier semestre 2023. Cela rend ce sujet plus pertinent et rend d'autant plus importante la connaissance des outils et technologies de prévention et de protection disponibles.

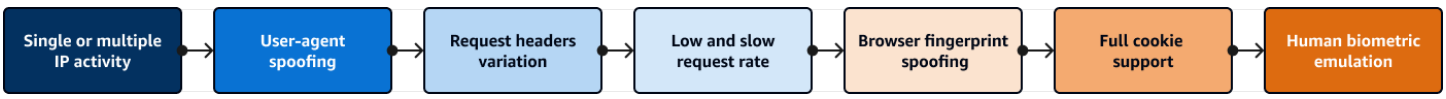
Le tableau suivant classe les différents types d'activité des robots et l'impact commercial que chacun d'entre eux peut avoir. Il ne s'agit pas d'une liste exhaustive ; il s'agit d'un résumé des activités les plus courantes des bots. Il souligne l'importance des contrôles de surveillance et d'atténuation. Pour une liste complète des menaces de bots, consultez le manuel de l'OWASP sur les menaces automatisées contre les applications (site Web de l'OWASP).

Type d'activité du bot	Description	Incidence potentielle
Grattage de contenu	Copie de contenus propriétaires destinés à être utilisés par des sites tiers	Impact sur votre référencement en raison de la duplication de contenu, de l'impact sur la marque et des problèmes de performance causés par des scrapers agressifs
bourrage d'informations d'identification	Test des bases de données d'informations d'identification volées sur votre site Web pour obtenir un accès ou valider des informations	Problèmes rencontrés par les utilisateurs, tels que les fraudes et les blocages de comptes, qui augmentent les demandes d'assistance et diminuent la confiance envers la marque
Craquage de cartes	Tester des bases de données contenant des données de cartes de crédit volées pour	Problèmes rencontrés par les utilisateurs, tels que le vol d'identité et la fraude, et la

Type d'activité du bot	Description	Incidence potentielle
	valider ou compléter les informations manquantes	détérioration de votre score de fraude
Déni de service	Augmenter le trafic vers un site Web spécifique pour ralentir la réponse ou le rendre indisponible pour le trafic légitime	Perte de revenus et atteinte à la réputation
Création de compte	Création de plusieurs comptes à des fins d'utilisation abusive ou de gain financier	Croissance entravée et analyses marketing biaisées
Scalping	Obtenir des biens en disponibilité limitée, souvent des billets, par rapport à de véritables consommateurs	Perte de revenus et problèmes pour les utilisateurs, tels que le manque d'accès aux biens vendus

Comment fonctionnent les botnets

Les tactiques, techniques et procédures (TTP) des opérateurs de botnets ont considérablement évolué au fil du temps. Ils ont dû suivre le rythme des technologies de détection et d'atténuation développées par les entreprises. La figure suivante illustre cette évolution. Au départ, les botnets utilisaient simplement les adresses IP comme moyen de fonctionnement, puis ils ont finalement évolué pour utiliser une émulation biométrique humaine sophistiquée. Cette sophistication coûte cher, et tous les botnets n'utilisent pas les outils les plus avancés. Il existe une combinaison d'opérateurs sur Internet, et ils évaluent probablement le meilleur outil pour le travail afin de fournir un bon retour sur investissement. L'un des objectifs de la défense contre les bots est de rendre l'activité du botnet coûteuse afin que la cible ne soit plus viable.



En général, les bots sont classés comme courants ou ciblés :

- Bots courants : ces robots s'identifient eux-mêmes et ne tenteront pas d'émuler les navigateurs. Nombre de ces robots exécutent des tâches utiles, telles que l'exploration du contenu, l'optimisation pour les moteurs de recherche (SEO) ou l'agrégation. Il est important d'identifier et de comprendre lesquels de ces robots courants arrivent sur votre site et quel effet ils ont sur votre trafic et vos performances.
- Bots ciblés — Ces robots tentent d'échapper à la détection en émulant les navigateurs. Ils utilisent des technologies de navigation, telles que les navigateurs headless, ou ils falsifient les empreintes digitales des navigateurs. Ils ont la capacité d'exécuter JavaScript et de prendre en charge les cookies. Leur intention n'est pas toujours claire et le trafic qu'ils génèrent peut ressembler à du trafic utilisateur normal.

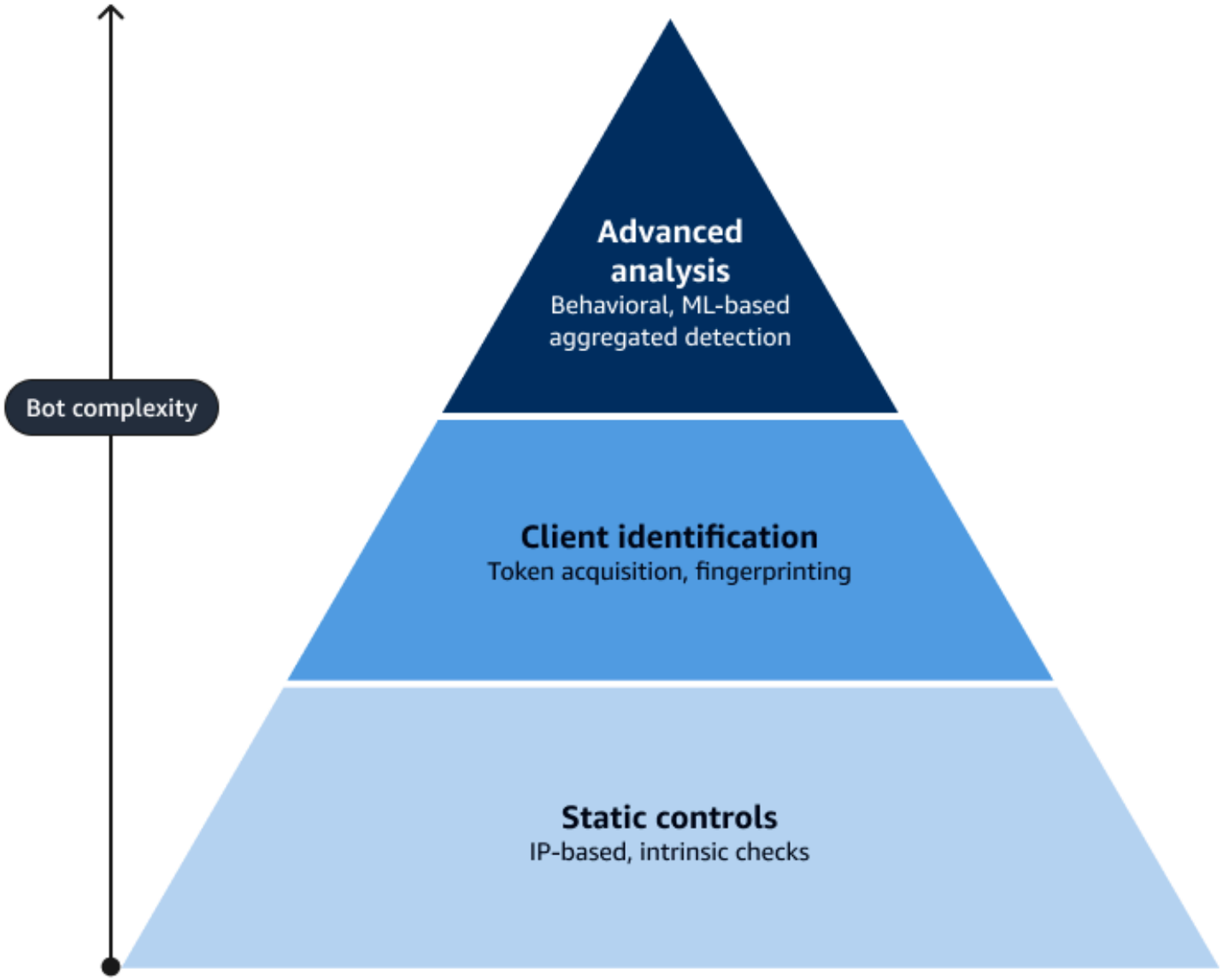
Les robots ciblés les plus avancés et les plus persistants imitent le comportement humain en générant des mouvements de souris et des clics semblables à ceux des humains sur un site Web. Ils sont les plus sophistiqués et les plus difficiles à détecter, mais ils sont également les plus coûteux à exploiter.

Souvent, un opérateur combine ces techniques. Cela crée un jeu de quête constante, dans lequel vous devez fréquemment modifier l'approche de protection et d'atténuation afin de vous adapter aux dernières techniques de l'opérateur. Ces robots sont considérés comme une menace persistante avancée (APT). Pour plus d'informations, consultez la section Menace persistante avancée dans le centre de ressources du NIST.

Techniques de contrôle des robots

L'objectif principal de l'atténuation des bots est de limiter l'impact négatif de l'activité des robots automatisés sur les sites Web, les services et les applications d'une organisation. La technologie et les techniques utilisées dépendent du type de trafic ou d'activité contre lequel vous souhaitez vous défendre. Pour y parvenir, il est essentiel de comprendre l'application et son trafic. Pour plus d'informations sur le point de départ, consultez la Directives pour le suivi de votre stratégie de contrôle des bots section de ce guide.

En général, les contrôles fournis par les solutions d'atténuation des bots peuvent être regroupés dans les catégories de haut niveau suivantes : statique, identification du client et analyse avancée. La figure suivante montre les différentes techniques disponibles et la manière dont elles peuvent être utilisées en fonction de la complexité de l'activité du bot. Cela montre comment la base, ou l'atténuation la plus large, peut être obtenue grâce à l'utilisation de contrôles statiques, tels que les listes d'autorisation et les vérifications intrinsèques. La plus petite partie de robots est toujours la plus avancée, et pour lutter contre ces robots, il faut une technologie plus avancée et une combinaison de contrôles.



Ensuite, ce guide explore chaque catégorie et ses techniques. Il décrit également les options disponibles AWS WAFpour implémenter ces contrôles :

- Contrôles statiques pour la gestion des robots
- Contrôles d'identification des clients pour la gestion des robots
- Contrôles d'analyse avancés pour la gestion des robots

Contrôles statiques pour la gestion des robots

Pour effectuer une action, les contrôles statiques évaluent les informations statiques de la requête HTTP (S), telles que son adresse IP ou ses en-têtes. Ces contrôles peuvent être utiles pour les

activités de robots peu sophistiquées ou pour le trafic bénéfique attendu de robots qui doit être vérifié et géré. Les techniques de contrôle statique incluent : les listes d'autorisations, les contrôles basés sur l'adresse IP et les contrôles intrinsèques.

Autoriser l'annonce

L'autorisation de mise en vente est un contrôle qui permet d'identifier le trafic convivial par le biais des contrôles d'atténuation des bots existants. Il existe différentes manières d'y parvenir. Le plus simple est d'utiliser une règle qui correspond à un ensemble d'adresses IP ou à une condition de correspondance similaire. Lorsqu'une demande correspond à une règle définie pour une `Allow` action, elle n'est pas évaluée par les règles suivantes. Dans certains cas, vous devez empêcher l'application de certaines règles uniquement ; en d'autres termes, vous devez autoriser la liste pour une règle, mais pas pour toutes les règles. Il s'agit d'un scénario courant de gestion des faux positifs pour les règles. L'autorisation de mise en vente est considérée comme une règle générale. Pour réduire le risque de faux négatifs, nous vous recommandons de l'associer à une autre option plus précise, telle qu'une correspondance de chemin ou d'en-tête.

Contrôles basés sur IP

Blocs d'adresses IP uniques

Un outil couramment utilisé pour atténuer l'impact des robots consiste à limiter les demandes provenant d'un seul demandeur. L'exemple le plus simple consiste à bloquer l'adresse IP source du trafic si ses demandes sont malveillantes ou si leur volume est élevé. Cela utilise des règles de correspondance des ensembles d' AWS WAF adresses IP pour implémenter des blocs basés sur l'adresse IP. Ces règles correspondent aux adresses IP et appliquent une action de `BlockChallenge`, ou`CAPTCHA`. Vous pouvez déterminer si un trop grand nombre de demandes proviennent d'une adresse IP en consultant le réseau de diffusion de contenu (CDN), un pare-feu d'applications Web ou les journaux des applications et des services. Cependant, dans la plupart des cas, ce contrôle n'est pas pratique sans automatisation.

L'automatisation des listes d'adresses IP bloquées se AWS WAF fait généralement à l'aide de règles basées sur le débit. Pour plus d’informations, consultez Règles basées sur un débit dans ce guide. Vous pouvez également implémenter les automatisations de sécurité pour la AWS WAF solution. Cette solution met automatiquement à jour la liste des adresses IP à bloquer, et une AWS WAF règle refuse les demandes correspondant à ces adresses IP.

L'un des moyens de reconnaître une attaque de bot consiste à faire en sorte qu'une multitude de requêtes provenant de la même adresse IP se concentrent sur un petit nombre de pages Web. Cela

indique que le bot supprime les prix ou tente à plusieurs reprises des connexions qui échouent à un pourcentage élevé. Vous pouvez créer des automatisations qui reconnaissent immédiatement ce modèle. Les automatisations bloquent l'adresse IP, ce qui réduit l'efficacité de l'attaque en l'identifiant et en l'atténuant rapidement. Le blocage d'adresses IP spécifiques est moins efficace lorsqu'un attaquant dispose d'un grand nombre d'adresses IP à partir desquelles lancer des attaques ou lorsque le comportement de l'attaque est difficile à reconnaître et à dissocier du trafic normal.

Réputation de l'adresse IP

Un service de réputation IP fournit des informations qui aident à évaluer la fiabilité d'une adresse IP. Ces informations sont généralement dérivées en agrégeant les informations relatives à l'IP provenant des activités passées à partir de cette adresse IP. Une activité antérieure permet d'indiquer dans quelle mesure une adresse IP est susceptible de générer des requêtes malveillantes. Les données sont ajoutées à des listes gérées qui suivent le comportement des adresses IP.

Les adresses IP anonymes constituent un cas spécifique de réputation des adresses IP. L'adresse IP source provient de sources connues d'adresses IP faciles à acquérir, telles que des machines virtuelles basées sur le cloud, ou de proxys, tels que des fournisseurs VPN ou des nœuds Tor connus. Les groupes de règles gérés par la liste de réputation d' AWS WAF Amazon IP et la liste d'adresses IP anonymes utilisent les renseignements internes d'Amazon sur les menaces pour identifier ces adresses IP.

Les informations fournies par ces listes gérées peuvent vous aider à agir sur les activités identifiées à partir de ces sources. Sur la base de ces informations, vous pouvez créer des règles qui bloquent directement le trafic ou des règles qui limitent le nombre de demandes (telles que des règles basées sur le débit). Vous pouvez également utiliser cette intelligence pour évaluer la source du trafic en utilisant les règles en `COUNT` mode. Cela examine les critères de correspondance et applique des étiquettes que vous pouvez utiliser pour créer des règles personnalisées.

Règles basées sur un débit

Les règles basées sur les taux peuvent être un outil précieux pour certains scénarios. Par exemple, les règles basées sur les taux sont efficaces lorsque le trafic des robots atteint des volumes élevés par rapport aux utilisateurs utilisant des identifiants de ressource uniformes (URI) sensibles ou lorsque le volume de trafic commence à affecter les opérations normales. La limitation du débit permet de maintenir les demandes à des niveaux gérables et de limiter et de contrôler l'accès. AWS WAF peut implémenter une règle de limitation de débit dans une liste de contrôle d'accès Web (ACL Web) en utilisant une instruction de règle basée sur le taux. Lorsque vous utilisez des règles basées sur le taux, il est recommandé d'inclure une règle générale couvrant l'ensemble du site, des règles

spécifiques aux URI et des règles basées sur le taux de réputation des adresses IP. Les règles basées sur le taux de réputation IP associent l'intelligence de la réputation des adresses IP à une fonctionnalité de limitation du débit.

Pour l'ensemble du site, une règle générale basée sur le taux de réputation des adresses IP crée un plafond qui empêche les robots peu sophistiqués d'inonder un site à partir d'un petit nombre d'adresses IP. La limitation du débit est particulièrement recommandée pour protéger les URI qui ont un coût ou un impact élevé, comme les pages de connexion ou de création de compte.

Les règles de limitation de débit peuvent fournir un premier niveau de défense rentable. Vous pouvez utiliser des règles plus avancées pour protéger les URI sensibles. Les règles basées sur le débit spécifiques aux URI peuvent limiter l'impact sur les pages critiques ou sur les API qui affectent le backend, telles que l'accès aux bases de données. Les mesures d'atténuation avancées visant à protéger certains URI, abordées plus loin dans ce guide, entraînent souvent des coûts supplémentaires, et ces règles basées sur les taux spécifiques aux URI peuvent vous aider à contrôler les coûts. Pour plus d'informations sur les règles basées sur les taux couramment recommandées, consultez les trois règles basées AWS WAF sur les taux les plus importantes dans le blog sur la AWS sécurité. Dans certains cas, il est utile de limiter le type de demande évalué par une règle basée sur le taux. Vous pouvez utiliser des instructions de portée réduite pour, par exemple, limiter les règles basées sur le taux en fonction de la zone géographique de l'adresse IP source.

AWS WAF offre une fonctionnalité avancée pour les règles basées sur les taux grâce à l'utilisation de clés d'agrégation. Grâce à cette fonctionnalité, vous pouvez configurer une règle basée sur le taux afin d'utiliser diverses autres clés d'agrégation et combinaisons de touches, en plus de l'adresse IP source. Par exemple, en tant que combinaison unique, vous pouvez agréger les demandes en fonction d'une adresse IP transférée, de la méthode HTTP et d'un argument de requête. Cela vous permet de configurer des règles plus précises pour une atténuation volumétrique sophistiquée du trafic.

Contrôles intrinsèques

Les contrôles intrinsèques sont différents types de validations ou de vérifications internes ou inhérentes au sein d'un système ou d'un processus. Pour le contrôle des robots, AWS WAF effectue une vérification intrinsèque en validant que les informations envoyées dans la demande correspondent aux signaux du système. Par exemple, il effectue des recherches DNS inversées et d'autres vérifications du système. Certaines demandes automatisées sont nécessaires, telles que les demandes liées au référencement. Autoriser la mise en vente est un moyen de laisser passer les bons robots attendus. Mais parfois, les robots malveillants imitent les bons robots, et il peut être

difficile de les séparer. AWS WAF fournit des méthodes pour y parvenir par le biais du groupe de règles AWS WAF Bot Control géré. Les règles de ce groupe permettent de vérifier que les robots auto-identifiés sont bien ceux qu'ils prétendent être. AWS WAF vérifie les détails de la demande par rapport au modèle connu de ce bot, et il effectue également des recherches DNS inversées et d'autres vérifications objectives.

Contrôles d'identification des clients pour la gestion des robots

Si le trafic lié à une attaque ne peut pas être facilement reconnu par le biais d'attributs statiques, la détection doit être en mesure d'identifier avec précision le client à l'origine de la demande. Par exemple, les règles basées sur le débit sont souvent plus efficaces et plus difficiles à contourner lorsque l'attribut limité au débit est spécifique à une application, tel qu'un cookie ou un jeton. L'utilisation d'un cookie lié à une session empêche les opérateurs de botnet de dupliquer des flux de demandes similaires entre de nombreux robots.

L'acquisition de jetons est couramment utilisée pour l'identification des clients. Pour l'acquisition de jetons, un JavaScript code collecte des informations pour générer un jeton qui est évalué côté serveur. L'évaluation peut aller de la vérification de ce qui JavaScript s'exécute sur le client à la collecte d'informations sur le périphérique pour la prise d'empreintes digitales. L'acquisition de jetons nécessite l'intégration d'un JavaScript SDK dans le site ou l'application, ou nécessite qu'un fournisseur de services effectue l'injection de manière dynamique.

Le fait d'avoir besoin d' JavaScript assistance constitue un obstacle supplémentaire pour les robots qui tentent d'émuler des navigateurs. Lorsqu'un SDK est impliqué, par exemple dans une application mobile, l'acquisition de jetons vérifie l'implémentation du SDK et empêche les robots d'imiter les requêtes de l'application.

L'acquisition de jetons nécessite l'utilisation de SDK implémentés côté client de la connexion. Les AWS WAF fonctionnalités suivantes fournissent un SDK JavaScript basé sur les navigateurs et un SDK basé sur des applications pour les appareils mobiles : Bot Control, prévention du rachat de compte Fraud Control (ATP) et prévention de la fraude lors de la création de comptes Fraud Control (ACFP).

Les techniques d'identification des clients incluent le CAPTCHA, le profilage du navigateur, l'empreinte digitale de l'appareil et l'empreinte TLS.

CAPTCHA

Le test public de Turing entièrement automatisé pour différencier les ordinateurs des humains (CAPTCHA) est utilisé pour distinguer les visiteurs robotiques des visiteurs humains et pour empêcher le scraping Web, le bourrage d'informations d'identification et le spam. Il existe une variété de mises en œuvre, mais elles impliquent souvent un casse-tête qu'un humain peut résoudre. Les CAPTCHA offrent une couche de défense supplémentaire contre les robots courants et peuvent réduire le nombre de faux positifs lors de la détection des robots.

AWS WAF permet aux règles d'exécuter une action CAPTCHA sur les requêtes Web qui répondent aux critères d'inspection d'une règle. Cette action est le résultat de l'évaluation des informations d'identification des clients collectées par le service. AWS WAF les règles peuvent nécessiter la résolution de problèmes CAPTCHA pour des ressources spécifiques fréquemment ciblées par des robots, telles que la connexion, la recherche et les soumissions de formulaires. AWS WAF peut directement servir le CAPTCHA par des moyens interstitiels ou en utilisant un SDK pour le gérer côté client. Pour plus d'informations, voir CAPTCHA et Challenge dans. AWS WAF

Profilage du navigateur

Le profilage du navigateur est une méthode de collecte et d'évaluation des caractéristiques du navigateur, dans le cadre de l'acquisition de jetons, afin de distinguer les vrais humains utilisant un navigateur interactif de l'activité des robots distribués. Vous pouvez établir un profilage de navigateur de manière passive par le biais des en-têtes, de l'ordre des en-têtes et d'autres caractéristiques des demandes inhérentes au fonctionnement des navigateurs.

Vous pouvez également effectuer le profilage du navigateur dans le code à l'aide de l'acquisition de jetons. En utilisant JavaScript le profilage du navigateur, vous pouvez rapidement déterminer si un client est compatible JavaScript. Cela vous permet de détecter les robots simples qui ne le supportent pas. Le profilage du navigateur ne se limite pas à vérifier les en-têtes et le JavaScript support HTTP ; le profilage du navigateur complique l'émulation complète d'un navigateur Web pour les robots. Les deux options de profilage du navigateur ont le même objectif : trouver des modèles dans un profil de navigateur qui indiquent une incohérence avec le comportement d'un navigateur réel.

AWS WAF le contrôle par bot pour les robots ciblés indique, dans le cadre de l'évaluation des jetons, si un navigateur présente des preuves d'automatisation ou des signaux incohérents. AWS WAF marque la demande afin d'effectuer l'action spécifiée dans la règle. Pour plus d'informations, consultez la section Détecter et bloquer le trafic des bots avancés dans le blog sur la AWS sécurité.

Empreinte digitale de l'appareil

L'empreinte digitale de l'appareil est similaire au profilage des navigateurs, mais elle ne se limite pas aux navigateurs. Le code exécuté sur un appareil (qui peut être un appareil mobile ou un navigateur Web) collecte et rapporte les détails de l'appareil à un serveur principal. Les détails peuvent inclure les attributs du système, tels que la mémoire, le type de processeur, le type de noyau du système d'exploitation (OS), la version du système d'exploitation et la virtualisation.

Vous pouvez utiliser les empreintes digitales de l'appareil pour savoir si un bot émule un environnement ou s'il existe des signes directs indiquant que l'automatisation est utilisée. En outre, les empreintes digitales de l'appareil peuvent également être utilisées pour reconnaître les demandes répétées provenant du même appareil.

La reconnaissance des demandes répétées provenant du même appareil, même si celui-ci essaie de modifier certaines caractéristiques de la demande, permet au système principal d'imposer des règles de limitation de débit. Les règles de limitation de débit basées sur l'empreinte digitale de l'appareil sont généralement plus efficaces que les règles de limitation de débit basées sur les adresses IP. Cela vous permet de limiter le trafic de bots qui alterne entre VPN ou proxys, mais qui provient d'un petit nombre d'appareils.

Lorsqu'il est utilisé avec des SDK d'intégration d'applications, AWS WAF le contrôle des robots ciblés peut agréger le comportement des demandes de session client. Cela vous permet de détecter et de séparer les sessions clients légitimes des sessions client malveillantes, même lorsque les deux proviennent de la même adresse IP. Pour plus d'informations sur le AWS WAF contrôle des bots pour les robots ciblés, consultez la section Détecter et bloquer le trafic des bots avancés dans le blog sur la AWS sécurité.

Empreinte TLS

Les empreintes digitales TLS, également connues sous le nom de règles basées sur les signatures, sont couramment utilisées lorsque les robots proviennent de nombreuses adresses IP mais présentent des caractéristiques similaires. Lors de l'utilisation du protocole HTTPS, le client et le serveur échangent des messages pour s'accuser réception et se vérifier mutuellement. Ils établissent des algorithmes cryptographiques et des clés de session. C'est ce qu'on appelle une poignée de main TLS. La façon dont une poignée de main TLS est mise en œuvre est une signature souvent utile pour reconnaître les attaques de grande envergure réparties sur de nombreuses adresses IP.

L'empreinte TLS permet aux serveurs Web de déterminer l'identité d'un client Web avec un haut degré de précision. Il ne nécessite que les paramètres de la première connexion par paquets, avant

tout échange de données d'application. Dans ce cas, le client Web fait référence à l'application qui lance une demande, qui peut être un navigateur, un outil CLI, un script (bot), une application native ou un autre client.

L'une des approches d'empreinte SSL et TLS est l'empreinte digitale JA3. JA3 enregistre une connexion client en fonction des champs du message Client Hello issu de la poignée de main SSL ou TLS. Il vous permet de profiler des clients SSL et TLS spécifiques sur différentes adresses IP sources, différents ports et différents certificats X.509.

Amazon CloudFront prend en charge l'ajout d'en-têtes JA3 aux demandes. Un `CloudFront-Viewer-JA3-Fingerprint` en-tête contient une empreinte de hachage de 32 caractères du paquet TLS Client Hello d'une demande d'affichage entrante. L'empreinte digitale encapsule les informations relatives à la façon dont le client communique. Ces informations peuvent être utilisées pour établir le profil des clients qui partagent le même schéma. Vous pouvez ajouter l'`CloudFront-Viewer-JA3-Fingerprinten`-tête à une politique de demande d'origine et associer cette politique à une CloudFront distribution. Vous pouvez ensuite inspecter la valeur de l'en-tête dans les applications d'origine ou dans Lambda @Edge et CloudFront Functions. Vous pouvez comparer la valeur de l'en-tête à une liste d'empreintes de logiciels malveillants connus pour bloquer les clients malveillants. Vous pouvez également comparer la valeur de l'en-tête à une liste d'empreintes attendues pour autoriser uniquement les demandes provenant de clients connus.

Contrôles d'analyse avancés pour la gestion des robots

Certains robots utilisent des outils de tromperie avancés pour échapper activement à la détection. Ces robots imitent le comportement humain afin d'effectuer une activité spécifique, telle que le scalping. Ces robots ont un but, et celui-ci est généralement lié à une grosse récompense monétaire.

Ces robots avancés et persistants utilisent une combinaison de technologies pour échapper à la détection ou se fondre dans le trafic normal. À son tour, cela nécessite également une combinaison de différentes technologies de détection pour identifier et atténuer avec précision le trafic malveillant.

Cas d'utilisation ciblés

Les données de cas d'utilisation peuvent fournir des opportunités de détection des robots. Les détections de fraudes sont des cas d'utilisation particuliers où des mesures d'atténuation spéciales sont justifiées. Par exemple, pour empêcher le piratage de comptes, vous pouvez comparer une liste de noms d'utilisateur et de mots de passe de comptes compromis avec les demandes de connexion ou de création de compte. Cela permet aux propriétaires de sites Web de détecter les tentatives

de connexion utilisant des informations d'identification compromises. L'utilisation d'informations d'identification compromises peut indiquer que des robots tentent de prendre le contrôle d'un compte ou que des utilisateurs ne savent pas que leurs informations d'identification sont compromises. Dans ce cas d'utilisation, les propriétaires de sites Web peuvent prendre des mesures supplémentaires pour vérifier l'identité de l'utilisateur, puis l'aider à modifier son mot de passe. AWS WAF fournit la règle gérée de prévention de la prise de contrôle des comptes (ATP) de Fraud Control pour ce cas d'utilisation.

Détection de bots agrégée ou au niveau de l'application

Certains cas d'utilisation nécessitent de combiner les données relatives aux demandes provenant du réseau de diffusion de contenu (CDN) et du backend de l'application ou du service. AWS WAF Parfois, vous devez même intégrer des informations tierces pour pouvoir prendre des décisions fiables concernant les robots.

Fonctionnalités d'Amazon CloudFront et AWS WAF peuvent envoyer des signaux à l'infrastructure principale, ou elles peuvent ensuite agréger les règles par le biais d'en-têtes et d'étiquettes. CloudFront expose les en-têtes d'empreintes digitales JA3, comme mentionné précédemment. Il s'agit d'un exemple de CloudFront fourniture de telles données par le biais d'un en-tête. AWS WAF peut envoyer des étiquettes lorsqu'elles correspondent à une règle. Les règles suivantes peuvent utiliser ces étiquettes pour prendre de meilleures décisions concernant les robots. Lorsque plusieurs règles sont combinées, vous pouvez implémenter des contrôles très précis. Un cas d'utilisation courant consiste à faire correspondre certaines parties d'une règle gérée par le biais d'une étiquette, puis à la combiner avec d'autres données de demande. Pour plus d'informations, consultez les exemples de correspondance d'étiquettes dans la AWS WAF documentation.

Analyse de l'apprentissage automatique

L'apprentissage automatique (ML) est une technique puissante pour traiter avec les robots. Le ML peut s'adapter à l'évolution des détails et, lorsqu'il est combiné à d'autres outils, constitue le moyen le plus robuste et le plus complet d'atténuer les bots avec un minimum de faux positifs. Les deux techniques de machine learning les plus courantes sont l'analyse comportementale et la détection des anomalies. Grâce à l'analyse comportementale, un système (dans le client, le serveur ou les deux) surveille la manière dont un utilisateur interagit avec l'application ou le site Web. Il surveille les mouvements de la souris ou la fréquence des interactions entre les clics et les touches. Le comportement est ensuite analysé à l'aide d'un modèle ML pour reconnaître les robots. La détection des anomalies est similaire. Il se concentre sur la détection de comportements ou de modèles significativement différents d'une base de référence définie pour l'application ou le site Web.

AWS WAF les contrôles ciblés pour les robots fournissent une technologie ML prédictive. Cette technologie permet de se défendre contre les attaques distribuées basées sur un proxy qui sont lancées par des robots conçus pour échapper à la détection. Le groupe de règles géréAWS WAF Bot Control utilise une analyse automatique automatique des statistiques de trafic du site Web pour détecter les comportements anormaux indiquant une activité de bot distribuée et coordonnée.

Déploiement et mise en œuvre de votre stratégie de contrôle des bots

Plusieurs facteurs doivent être pris en compte lors de la planification d'une stratégie de déploiement de contrôle des bots. Outre les caractéristiques uniques des applications Web, la taille de l'environnement, le processus de développement et la structure organisationnelle influent sur la stratégie de déploiement. En fonction de votre environnement et des caractéristiques de votre application, une stratégie de déploiement centralisée ou décentralisée peut être utilisée :

- Stratégie de déploiement centralisée — Une approche centralisée permet un degré de contrôle plus élevé lorsque vous souhaitez appliquer strictement le contrôle des bots. Cette approche convient parfaitement si les équipes d'application préfèrent décharger la gestion. Une approche centralisée est particulièrement efficace lorsque les applications Web présentent des caractéristiques similaires. Dans ce cas, les applications bénéficient d'un ensemble commun de règles de contrôle des bots et de mesures d'atténuation des bots.
- Stratégie de déploiement décentralisée — Une approche décentralisée donne aux équipes d'application l'autonomie nécessaire pour définir et mettre en œuvre des configurations de contrôle des bots de manière indépendante. Cette approche est courante dans les environnements de petite taille ou lorsque les équipes d'application doivent garder le contrôle de leurs politiques de contrôle des bots. En raison de la nature de nombreuses applications Web, il est souvent nécessaire de maintenir des politiques de contrôle des bots indépendantes adaptées aux caractéristiques uniques des applications, ce qui entraîne une approche décentralisée.
- Stratégie combinée — La combinaison de ces deux approches est appropriée pour une combinaison d'applications Web. Par exemple, cela peut impliquer un ensemble de règles de base qui s'appliquent à toutes les ACL Web, tandis que la gestion de politiques de contrôle des bots plus spécifiques est déléguée aux équipes d'application.

Vous pouvez l'utiliser AWS Firewall Managerpour centraliser et automatiser le déploiement des ACL AWS WAF Web qui définissent les politiques de contrôle des robots. Lorsque vous utilisez Firewall Manager, déterminez s'il est approprié de centraliser les politiques de contrôle des bots, notamment si elles doivent être déléguées aux équipes chargées des applications. Avec Firewall Manager, vous pouvez utiliser le balisage pour permettre aux équipes chargées des applications d'accepter des AWS WAF politiques. Cela fournit AWS WAF une fonctionnalité intelligente d'atténuation des menaces. Vous pouvez également activer la AWS WAF journalisation centralisée pour les applications et les opérations de sécurité.

Quelle que soit la stratégie de déploiement utilisée, il est recommandé de définir et de gérer le processus d'intégration par le biais de frameworks basés sur l'infrastructure en tant que code (IaC), tels que AWS CloudFormationou le AWS Cloud Development Kit (AWS CDK). Cela vous permet de configurer le contrôle de source pour stocker et versionner les objets de configuration. Pour plus d'informations, consultez les exemples de AWS WAF configuration pour AWS CDK(GitHub) et CloudFormation(AWS documentation).

Stratégie de mise en œuvre

Une fois que vous avez sélectionné une stratégie de déploiement, la mise en œuvre peut commencer. La stratégie de déploiement définit la manière dont les règles sont déployées pour les différentes applications. Dans la stratégie de mise en œuvre, l'accent est mis sur le processus itératif d'ajout de contrôles, de tests, de surveillance continue, puis d'évaluation de leurs effets.

Comprendre les modèles de trafic

Pour bien comprendre les modèles de trafic, il est important de vous familiariser avec le fonctionnement métier de l'application et les attributs attendus, tels que les modèles d'utilisation, les ressources clés et les profils des utilisateurs. Intégrez le trafic de production et le trafic généré lors des tests par rapport à l'application afin d'établir une base de référence pour l'évaluation. Assurez-vous que la période inclut des données de trafic qui représentent suffisamment les multiples pics d'utilisation.

À l'aide de votre outil préféré, consultez les journaux de trafic et les statistiques sur la période d'utilisation représentative. Analysez les données du AWS WAF journal pour détecter les demandes anormales en filtrant les champs du journal tels que `headers` (par exemple, `User-Agent` et`Referer`)`country`, et`clientIp`. Prenez note des identifiants de ressources uniformes (URI) et de leur fréquence d'accès. Catégorisez le trafic, par exemple en identifiant les bons robots. Par exemple, autorisez l'accès à des robots utiles, tels que les robots d'exploration et les moniteurs des moteurs de recherche.

Dans la AWS WAF console, sur le tableau de bord de contrôle des bots, un échantillon de l'activité des bots est disponible pour toute ACL Web active. Bien que cela fournisse un premier aperçu des volumes courants de demandes de robots, effectuez une configuration et une analyse supplémentaires pour mieux comprendre l'activité des robots.

Pour une mise en œuvre efficace, vous devez bien comprendre le trafic des robots, ses effets et savoir quelles demandes de bot sont bénéfiques ou malveillantes. Cela facilite la phase suivante, à savoir la sélection des contrôles, et vous permet d'évaluer le trafic des bots en parallèle.

Sélection et ajout de contrôles

L'analyse initiale du trafic permet de déterminer les commandes de bot à utiliser et les actions à sélectionner pour chacune d'entre elles. Vous pouvez également choisir d'enregistrer et de surveiller l'activité en vue d'éventuelles actions futures. L'analyse initiale du trafic vous aide à sélectionner le meilleur contrôle pour gérer le trafic. Pour plus d'informations sur les commandes disponibles, consultez Techniques de contrôle des robots ce guide.

Envisagez d'inclure des implémentations de SDK supplémentaires au cours de cette étape. Cela vous permet de tester et de terminer les implémentations du SDK dans toutes les applications requises. AWS WAF les règles de contrôle des bots et de lutte contre la fraude offrent un avantage complet en matière d'évaluation des jetons lorsque vous implémentez un JavaScript SDK ou un SDK mobile. Pour plus d'informations, consultez la section Pourquoi utiliser les SDK d'intégration d'applications avec Bot Control dans la AWS WAF documentation.

Nous recommandons d'implémenter l'acquisition de jetons pour différents types d'applications comme suit :

- Application monopage (SPA) — JavaScript SDK (pas de redirection)
- Navigateur mobile : JavaScript SDK ou actions de règles (CAPTCHA ou Challenge)
- Vues Web : JavaScript SDK ou actions de règles (CAPTCHA ou Challenge)
- Applications natives — SDK mobile
- iFrames — SDK JavaScript

Pour plus d'informations sur la mise en œuvre des SDK, consultez la section Intégration des applications AWS WAF clientes dans la AWS WAF documentation.

Test et déploiement en production

Les contrôles doivent être initialement déployés dans un environnement hors production où vous pouvez effectuer des tests pour vérifier que les fonctionnalités attendues de l'application Web sont préservées. Effectuez toujours une validation complète dans un environnement de test avant le déploiement en production.

Après les tests et la validation dans un environnement hors production, la version de production peut être lancée. Sélectionnez la date et l'heure auxquelles le trafic utilisateur attendu est le plus faible. Avant le déploiement, les équipes chargées des applications et de la sécurité doivent examiner l'état

de préparation opérationnelle, discuter de la manière d'annuler les modifications et examiner les tableaux de bord pour s'assurer que toutes les mesures et alarmes requises sont configurées.

Avec le déploiement CloudFront continu d'Amazon, vous pouvez envoyer une petite quantité de trafic vers une distribution intermédiaire dotée d'une ACL AWS WAF Web configurée spécifiquement pour l'évaluation du contrôle des robots. AWS WAF assure la gestion des versions de toutes les règles gérées nouvelles ou mises à jour afin que vous puissiez tester et approuver les modifications avant qu'elles ne commencent à évaluer le trafic de production.

Évaluation et réglage des commandes

Les contrôles mis en œuvre peuvent fournir un aperçu et une visibilité supplémentaires de l'activité et des modèles de trafic. Surveillez et analysez fréquemment le trafic des applications afin d'ajouter ou d'ajuster des contrôles de sécurité. Il y a normalement une phase de réglage pour atténuer les éventuels faux négatifs et faux positifs. Les faux négatifs sont des attaques qui n'ont pas été détectées par vos contrôles et qui vous obligent à durcir vos règles. Les faux positifs représentent des demandes légitimes qui ont été identifiées à tort comme des attaques et bloquées en conséquence.

L'analyse et le réglage peuvent être effectués manuellement ou à l'aide d'outils. Un système de gestion des informations et des événements de sécurité (SIEM) est un outil courant qui permet de fournir des métriques et une surveillance intelligente. Il en existe plusieurs, plus ou moins sophistiqués, mais ils constituent tous un bon point de départ pour obtenir des informations sur le trafic.

La définition d'indicateurs clés de performance (KPI) importants pour les sites Web et les applications peut vous aider à identifier plus rapidement les dysfonctionnements attendus. Par exemple, vous pouvez utiliser les rétrofacturations par carte de crédit, les ventes par compte ou les taux de conversion comme indicateurs d'anomalies commerciales pouvant être générées par des robots. Il est encore plus important de définir et de comprendre quels indicateurs et indicateurs de performance clés il est utile de surveiller que le simple fait de surveiller.

Comprendre comment obtenir les bons indicateurs et les bons journaux à partir d'une solution de contrôle des bots est tout aussi important que d'identifier les indicateurs à surveiller. La section suivante détaille Directives pour le suivi de votre stratégie de contrôle des bots les options de surveillance et de visibilité à prendre en compte.

Directives pour le suivi de votre stratégie de contrôle des bots

Pour le trafic des bots et le trafic des applications Web, la surveillance et la visibilité revêtent une grande importance. Il vous aide à hiérarchiser les activités ainsi que les opérations de sécurité. Si la journalisation détaillée ou l'utilisation d'un système SIEM ne sont pas possibles, un bon point de départ consiste à surveiller les indicateurs de base fournis par la solution ou le fournisseur que vous avez sélectionné.

Cette visibilité est utile pour les informations sur les menaces, le renforcement des règles, le dépannage des faux positifs et la réponse à un incident. Plusieurs options de surveillance sont disponibles avec AWS WAF. Pour une surveillance de haut niveau, AWS WAF fournit des informations générales sur le trafic dans le AWS Management Console. Ceci est disponible pour l'ensemble du trafic ainsi qu'une vue détaillée pour le trafic des bots, lorsque le groupe de règles Bot Control est activé dans votre ACL Web.

AWS WAF fournit différentes options pour la journalisation détaillée du trafic ACL Web. Vous pouvez également ajouter des étiquettes aux demandes, que vous pouvez utiliser pour faciliter l'analyse des journaux et configurer les règles d'évaluation des robots. En intégrant Amazon CloudWatch Logs Insights, vous pouvez interroger les AWS WAF journaux et visualiser les résultats.

Si vous activez la journalisation détaillée, cela AWS WAF fournit une visibilité supplémentaire au-delà du tableau de bord de contrôle des bots préconfiguré. L'utilisation de AWS WAF journaux pour visualiser le trafic, ainsi que d'enquêtes ad hoc, peut fournir une compréhension approfondie des modèles de trafic et des options d'atténuation pour une application Web.

Vous pouvez intégrer les données des AWS WAF CloudWatch journaux à Amazon Logs, Amazon Simple Storage Service (Amazon S3) ou Amazon Data Firehose. Pour plus d'informations, consultez Activer la AWS WAF journalisation et envoyer des journaux à CloudWatch Amazon S3 ou Amazon Data Firehose. Vous pouvez également envoyer des journaux à différentes cibles à des fins d'analyse, notamment à Amazon OpenSearch Service ou à une AWS Marketplacesolution. Pour plus d'informations, consultez la section Paramètres de destination dans la documentation de Firehose. Si plusieurs sources de journaux sont utilisées, une solution de journalisation centralisée est recommandée pour corréler les sources.

Ensuite, ce guide fournit des recommandations sur la manière de commencer à surveiller le trafic des bots et de gagner en visibilité en utilisant Amazon CloudWatch.

Règles de suivi les plus importantes

Le suivi des règles les plus utilisées peut mettre en évidence les tendances et les activités potentiellement anormales. L'augmentation des taux pour une règle spécifique peut indiquer un faux positif potentiel ou une activité ciblée que vous devriez étudier. La règle de suivi la plus courante serait Contrôles basés sur IP les règles de blocage géographique (un pic ici peut indiquer du trafic provenant de pays inhabituels, qui ne sont peut-être pas automatiquement bloqués), et. Règles basées sur un débit Ces règles présentent toujours des variations inhérentes, mais une anomalie dans le schéma de trafic peut indiquer l'activité d'un bot. Tenez-en compte si vous définissez les seuils manuellement.

Suivi des principaux labels et espaces de noms

En utilisant CloudWatch des métriques pour suivre les principaux labels, vous pouvez voir quelles AWS WAF règles sont fréquemment invoquées. Cela vous permet de détecter les anomalies, telles qu'une augmentation de l'activité des scraper, du trafic provenant de sources suspectes ou une tentative d'utilisation abusive de la page de connexion ou de l'API de l'application.

Voici des exemples d'étiquettes susceptibles de vous intéresser :

- `awswaf:managed:aws:bot-control:signal:non_browser_user_agent`
- `awswaf:managed:aws:bot-control:bot:category:http_library`
- `awswaf:managed:aws:bot-control:bot:name:curl`
- `awswaf:managed:aws:atp:signal:credential_compromised`
- `awswaf:managed:aws:core-rule-set:NoUserAgent_Header`
- `awswaf:managed:token:rejected`

Voici des exemples d'espaces de noms d'étiquettes susceptibles de vous intéresser :

- `awswaf:managed:aws:bot-control:`
- `awswaf:managed:aws:atp:`
- `awswaf:managed:aws:anonymous-ip-list:`

Création d'expressions mathématiques

Dans Amazon CloudWatch, vous pouvez créer des expressions mathématiques pour une ou toutes les règles. Si vous définissez des alertes sur des expressions mathématiques, vous serez averti des anomalies des taux, et non des quantités, de certaines mesures. Il s'agit d'un outil important pour réduire la fatigue liée aux alertes.

Créez une métrique personnalisée basée sur une expression mathématique. Examinez les taux relatifs des règles par rapport au nombre total de demandes adressées à une application. Voici une expression mathématique courante :

```
[ruleX count * 100]/[All allowed requests + All blocked requests]
```

Cette expression mathématique fournit un pourcentage qui vous permet de suivre une règle spécifique et de visualiser son évolution dans le temps.

Utilisation de la détection d'anomalies

L'utilisation de la détection des CloudWatch anomalies sur n'importe quel CloudWatch indicateur peut fournir des alertes sur des tendances anormalement basses ou élevées, sans définir manuellement le seuil réel. Ces algorithmes analysent en permanence les métriques des systèmes et des applications, déterminent les bases de référence normales et détectent les anomalies avec une intervention minimale de l'utilisateur. CloudWatch applique des algorithmes statistiques et ML dans sa fonction de détection des anomalies.

Utilisation des CloudWatch métriques Amazon

AWS WAF traite le trafic et ajoute des étiquettes aux demandes qui correspondent aux règles définies dans l'ACL Web. Chaque étiquette crée une métrique dans CloudWatch. Dans le même temps, chaque règle ACL Web crée également des métriques pour chacune de ses actions possibles. Utilisez ces indicateurs d'étiquette et d'action pour mieux comprendre le trafic des bots. Il s'agit d'une approche rentable pour visualiser les tendances. Pour plus d'informations, voir Afficher les métriques disponibles et Représentation graphique des métriques dans la CloudWatch documentation.

CloudWatch offre la possibilité d'envoyer des données à un collecteur de journaux ou à un agrégateur, qu'il s'agisse d'une solution tierce Service AWS ou d'une solution tierce. L'ingestion de données provenant de CloudWatch peut fournir une expérience d'observabilité de sécurité plus

consolidée, grâce à laquelle vous pouvez corréler des données provenant de plusieurs sources. Cela peut vous aider à étudier, visualiser ou configurer vos alertes et vos automatisations de sécurité.

Création d'un tableau de bord

Après avoir identifié les indicateurs importants à suivre, créez un tableau de bord contenant les indicateurs les plus pertinents. Les afficher sous une seule vitre peut apporter une visibilité et un contrôle supplémentaires. side-by-side

Il est toujours préférable de configurer des alertes et des règles d'automatisation pour les valeurs métriques anormales. Ne vous fiez pas aux humains pour identifier les anomalies en consultant un tableau de bord. Cependant, les tableaux de bord peuvent être utiles à des fins d'enquête après réception d'une alerte.

Optimisation des coûts pour votre stratégie de contrôle des bots

La nature du trafic Web est dynamique. Cela signifie que la technologie et les services utilisés pour atténuer les menaces peuvent varier et être ajustés au fil du temps. C'est essentiel lorsque l'on considère une stratégie de contrôle des robots et les contrôles qu'elle inclut. L'optimisation au fil du temps est le principal principe à garder à l'esprit, et il provient du pilier d'optimisation des coûts du AWS Well-Architected Framework.

AWS WAF Les ACL Web peuvent être dynamiques, en particulier lorsque de nouvelles fonctionnalités sont publiées ou lorsque vous essayez d'atténuer une nouvelle menace. Pour garder un œil sur vos coûts, vous devez comprendre les dimensions du coût du AWS WAF service et la façon dont chacune affecte vos dépenses finales. Le principal coût moteur est le nombre de demandes évaluées par le service. Des frais supplémentaires s'appliquent si vous utilisez les groupes de règles gérés par Bot Control et Account Takeover Prevention (ATP) ou si vous utilisez des actions avancées, telles que le CAPTCHA ou le challenge.

Les contrôles par bots spécialisés étant onéreux, le principal objectif d'optimisation des coûts est de réduire le nombre de demandes inspectées par ces contrôles avancés. Les techniques applicables incluent la séparation des contenus de grande valeur, l'application d'abord de mesures moins coûteuses, la délimitation du domaine d'évaluation et la combinaison de la protection contre les robots avec d'autres types de contrôles. Les techniques de surveillance des coûts offrent une visibilité supplémentaire au sein de votre organisation.

Séparer le contenu dynamique du contenu statique

L'une des techniques de réduction des coûts consiste à isoler le contenu statique de l'application dynamique. La majorité des demandes adressées à des applications Web classiques sont des demandes adressées à des objets statiques. Une méthode courante pour réduire la charge sur les serveurs d'applications consiste à déplacer le contenu statique vers sa propre URL, par exemple`static.example.com`. Cela est souvent réalisé en créant une distribution de contenu unique avec une configuration de mise en cache optimisée pour le contenu statique. Cette technique peut également contribuer à réduire les coûts de contrôle des bots si le contenu statique n'est pas couramment ciblé sur le site ou l'application. La séparation du contenu statique de l'application dynamique peut permettre une application plus précise des contrôles avancés des bots.

Appliquer d'abord les règles de réduction des coûts

Une autre technique consiste à appliquer des règles de base moins coûteuses qui filtrent le trafic indésirable avant d'utiliser des contrôles avancés, qui sont plus coûteux. Dans la pratique, cela implique généralement de placer les mesures d'atténuation du contrôle des bots comme dernière couche de défense et d'utiliser les contrôles précédents pour filtrer le trafic indésirable. Cette approche pyramidale a déjà été abordée Techniques de contrôle des robots dans ce guide. L'objectif principal est d'utiliser ces options moins coûteuses pour arrêter le trafic indésirable, ce qui réduit le nombre de demandes traitées par des techniques d'atténuation avancées et plus coûteuses.

Délimitation du domaine d'évaluation

AWS WAF les instructions scope-down constituent une technique puissante pour réduire le nombre de demandes inspectées par des règles avancées. Si la séparation du contenu statique dans sa propre URL ne peut pas être implémentée, les instructions scope-down constituent une autre méthode pour filtrer les demandes qui ne nécessitent pas de techniques d'atténuation avancées. Cela peut être fait en définissant un chemin d'application spécifique, une méthode HTTP (telle que POST) ou une combinaison similaire.

Combiner la protection contre les robots avec d'autres contrôles

Des considérations supplémentaires en matière de contrôle des coûts doivent être prises en compte lors de la protection des applications contre de multiples menaces, en plus du trafic de bots indésirable. Par exemple, la protection contre les attaques par déni de service distribué (DDoS) et contre le piratage de comptes nécessite une configuration supplémentaire susceptible d'avoir une incidence sur les coûts. Shield Advanced est recommandé pour protéger les applications contre les attaques DDoS. En particulier, ses mesures d'atténuation au niveau de la couche applicative peuvent automatiquement répondre aux inondations de demandes, réduisant ainsi le nombre de demandes susceptibles d'être traitées par le groupe de règles AWS WAF Bot Control, lorsque la règle est placée en tête dans l'ordre d'évaluation. Shield Advanced présente un avantage supplémentaire : les AWS WAF règles standard gérées et personnalisées sont gratuites pour les ressources protégées par Shield Advanced. Notez que les groupes de règles d'atténuation intelligente des menaces, notamment Bot Control, entraînent des coûts supplémentaires, même pour les ressources protégées par Shield Advanced.

Les applications qui nécessitent une prévention du piratage de compte peuvent utiliser le groupe de règles de prévention du piratage de compte (ATP) AWS WAF Fraud Control. Le coût d'inspection par

demande du groupe de règles ATP est supérieur à celui du groupe de règles Bot Control. En raison de ce coût plus élevé, il est essentiel d'appliquer le groupe de règles ATP aussi précisément que possible. L'utilisation du groupe de règles Bot Control en conjonction avec ATP peut aider à atteindre cet objectif. Le groupe de règles Bot Control doit être placé avant ATP dans l'ACL Web afin de filtrer les demandes de bot et de réduire le nombre de demandes inspectées par ATP.

Pour une optimisation continue, l'activité la plus importante consiste à surveiller CloudWatchles métriques associées au groupe de règles Bot Control. Au fil du temps, l'objectif est de réduire le nombre de demandes évaluées par le groupe de règles Bot Control afin de limiter le nombre de demandes qui ciblent les ressources dont vous avez besoin pour vous protéger contre les activités indésirables des bots. La création CloudWatch de tableaux de bord fournit une visibilité sur les indicateurs les plus critiques pour les applications, notamment AWS WAF les coûts et l'utilisation.

Coûts de surveillance

AWS Cost Explorer est un outil qui vous permet d'afficher et d'analyser vos coûts et l'utilisation. Cost Explorer facilite l'analyse des AWS coûts, y compris AWS WAF les coûts engagés. L'outil fournit des informations sur les coûts pour les 12 derniers mois et prévoit les dépenses futures pour les 12 prochains mois.

AWS La détection des anomalies de coûts est un autre outil de contrôle des coûts qui peut être utile pour surveiller les AWS WAF coûts. Il utilise des technologies de machine learning avancées pour identifier les dépenses anormales et les causes profondes. Cela vous permet d'agir rapidement ou de recevoir des alertes en cas d'augmentation inattendue des coûts. Pour recevoir une alerte lorsqu'un seuil de coût spécifique est atteint, AWS Budgetsvous pouvez fournir cette fonctionnalité de suivi et de surveillance.

Ressources

AWS documentation

- AWS WAF guide du développeur
- AWS Meilleures pratiques en matière de résilience aux attaques DDoS (livres blancs)AWS
- Directives de mise en œuvre AWS WAF (AWS livres blancs)

Autres AWS ressources

- Analyse AWS WAF des journaux dans Amazon CloudWatch Logs (article de AWS blog)
- Déployez un tableau de bord AWS WAF avec un minimum d'effort (article de AWS blog)
- Automatisations de sécurité pour AWS WAF (bibliothèque de AWS solutions)
- Les trois règles les plus importantes AWS WAF basées sur les taux (article de AWS blog)
- Visualisez AWS WAF les journaux avec un CloudWatch tableau de bord Amazon (article de AWS blog)

Collaborateurs

Conception

- Diana Alvarado, architecte de solutions senior, AWS
- Cameron Worrell, architecte d'entreprise, AWS
- Geary Scherer, architecte de solutions, AWS
- Tzoori Tamam, architecte de solutions principal, AWS

Révision

- Jess Izen, ingénieure senior en développement logiciel, AWS
- Kaustubh Phatak, chef de produit senior, AWS
- Vikramaditya Bhatnagar, consultant principal en sécurité, AWS

Rédaction technique

- Lilly AbouHarb, rédactrice technique senior, AWS

Historique du document

Le tableau suivant décrit les modifications importantes apportées à ce guide. Pour être averti des mises à jour à venir, abonnez-vous à un fil RSS.

Modification	Description	Date
Publication initiale	—	21 février 2024

AWS Glossaire des directives prescriptives

Les termes suivants sont couramment utilisés dans les stratégies, les guides et les modèles fournis par les directives AWS prescriptives. Pour suggérer des entrées, veuillez utiliser le lien Faire un commentaire à la fin du glossaire.

Nombres

7 R

Sept politiques de migration courantes pour transférer des applications vers le cloud. Ces politiques s'appuient sur les 5 R identifiés par Gartner en 2011 et sont les suivantes :

- Refactorisation/réarchitecture : transférez une application et modifiez son architecture en tirant pleinement parti des fonctionnalités natives cloud pour améliorer l'agilité, les performances et la capacité de mise à l'échelle. Cela implique généralement le transfert du système d'exploitation et de la base de données. Exemple : migrez votre base de données Oracle sur site vers l'édition compatible avec Amazon Aurora PostgreSQL.
- Replateformer (déplacer et remodeler) : transférez une application vers le cloud et introduisez un certain niveau d'optimisation pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle sur site vers Amazon Relational Database Service (Amazon RDS) pour Oracle dans le. AWS Cloud
- Racheter (rachat) : optez pour un autre produit, généralement en passant d'une licence traditionnelle à un modèle SaaS. Exemple : migrez votre système de gestion de la relation client (CRM) vers Salesforce.com.
- Réhéberger (lift and shift) : transférez une application vers le cloud sans apporter de modifications pour tirer parti des fonctionnalités du cloud. Exemple : migrez votre base de données Oracle locale vers Oracle sur une EC2 instance du AWS Cloud.
- Relocaliser (lift and shift au niveau de l'hyperviseur) : transférez l'infrastructure vers le cloud sans acheter de nouveau matériel, réécrire des applications ou modifier vos opérations existantes. Vous migrez des serveurs d'une plateforme sur site vers un service cloud pour la même plateforme. Exemple : migrer une Microsoft Hyper-V application vers AWS.
- Retenir : conservez les applications dans votre environnement source. Il peut s'agir d'applications nécessitant une refactorisation majeure, que vous souhaitez retarder, et d'applications existantes que vous souhaitez retenir, car rien ne justifie leur migration sur le plan commercial.

- Retirer : mettez hors service ou supprimez les applications dont vous n'avez plus besoin dans votre environnement source.

A

ABAC

Voir contrôle d'accès basé sur les attributs.

services abstraits

Consultez la section Services gérés.

ACIDE

Voir atomicité, consistance, isolation, durabilité.

migration active-active

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue (à l'aide d'un outil de réplication bidirectionnelle ou d'opérations d'écriture double), tandis que les deux bases de données gèrent les transactions provenant de la connexion d'applications pendant la migration. Cette méthode prend en charge la migration par petits lots contrôlés au lieu d'exiger un basculement ponctuel. Elle est plus flexible mais demande plus de travail qu'une migration active-passive.

migration active-passive

Méthode de migration de base de données dans laquelle la synchronisation des bases de données source et cible est maintenue, mais seule la base de données source gère les transactions provenant de la connexion d'applications pendant que les données sont répliquées vers la base de données cible. La base de données cible n'accepte aucune transaction pendant la migration.

fonction d'agrégation

Fonction SQL qui agit sur un groupe de lignes et calcule une valeur de retour unique pour le groupe. Des exemples de fonctions d'agrégation incluent `SUM` et`MAX`.

AI

Voir intelligence artificielle.

AIOps

Voir les opérations d'intelligence artificielle.

anonymisation

Processus de suppression définitive d'informations personnelles dans un ensemble de données. L'anonymisation peut contribuer à protéger la vie privée. Les données anonymisées ne sont plus considérées comme des données personnelles.

anti-motif

Solution fréquemment utilisée pour un problème récurrent lorsque la solution est contre-productive, inefficace ou moins efficace qu'une alternative.

contrôle des applications

Une approche de sécurité qui permet d'utiliser uniquement des applications approuvées afin de protéger un système contre les logiciels malveillants.

portefeuille d'applications

Ensemble d'informations détaillées sur chaque application utilisée par une organisation, y compris le coût de génération et de maintenance de l'application, ainsi que sa valeur métier. Ces informations sont essentielles pour le processus de découverte et d'analyse du portefeuille et permettent d'identifier et de prioriser les applications à migrer, à moderniser et à optimiser.

intelligence artificielle (IA)

Domaine de l'informatique consacré à l'utilisation des technologies de calcul pour exécuter des fonctions cognitives généralement associées aux humains, telles que l'apprentissage, la résolution de problèmes et la reconnaissance de modèles. Pour plus d'informations, veuillez consulter Qu'est-ce que l'intelligence artificielle ?

opérations d'intelligence artificielle (AIOps)

Processus consistant à utiliser des techniques de machine learning pour résoudre les problèmes opérationnels, réduire les incidents opérationnels et les interventions humaines, mais aussi améliorer la qualité du service. Pour plus d'informations sur son AIOps utilisation dans la stratégie de AWS migration, consultez le guide d'intégration des opérations.

chiffrement asymétrique

Algorithme de chiffrement qui utilise une paire de clés, une clé publique pour le chiffrement et une clé privée pour le déchiffrement. Vous pouvez partager la clé publique, car elle n'est pas utilisée pour le déchiffrement, mais l'accès à la clé privée doit être très restreint.

atomicité, cohérence, isolement, durabilité (ACID)

Ensemble de propriétés logicielles garantissant la validité des données et la fiabilité opérationnelle d'une base de données, même en cas d'erreur, de panne de courant ou d'autres problèmes.

contrôle d'accès par attributs (ABAC)

Pratique qui consiste à créer des autorisations détaillées en fonction des attributs de l'utilisateur, tels que le service, le poste et le nom de l'équipe. Pour plus d'informations, consultez ABAC pour AWS dans la documentation AWS Identity and Access Management (IAM).

source de données faisant autorité

Emplacement où vous stockez la version principale des données, considérée comme la source d'information la plus fiable. Vous pouvez copier les données de la source de données officielle vers d'autres emplacements à des fins de traitement ou de modification des données, par exemple en les anonymisant, en les expurgant ou en les pseudonymisant.

Zone de disponibilité

Un emplacement distinct au sein d'un Région AWS réseau isolé des défaillances dans d'autres zones de disponibilité et fournissant une connectivité réseau peu coûteuse et à faible latence aux autres zones de disponibilité de la même région.

AWS Cadre d'adoption du cloud (AWS CAF)

Un cadre de directives et de meilleures pratiques visant AWS à aider les entreprises à élaborer un plan efficace pour réussir leur migration vers le cloud. AWS La CAF organise ses conseils en six domaines prioritaires appelés perspectives : les affaires, les personnes, la gouvernance, les plateformes, la sécurité et les opérations. Les perspectives d'entreprise, de personnes et de gouvernance mettent l'accent sur les compétences et les processus métier, tandis que les perspectives relatives à la plateforme, à la sécurité et aux opérations se concentrent sur les compétences et les processus techniques. Par exemple, la perspective liée aux personnes cible les parties prenantes qui s'occupent des ressources humaines (RH), des fonctions de dotation en personnel et de la gestion des personnes. Dans cette perspective, la AWS CAF fournit des conseils pour le développement du personnel, la formation et les communications afin de préparer l'organisation à une adoption réussie du cloud. Pour plus d'informations, veuillez consulter le site Web AWS CAF et le livre blanc AWS CAF.

AWS Cadre de qualification de la charge de travail (AWS WQF)

Outil qui évalue les charges de travail liées à la migration des bases de données, recommande des stratégies de migration et fournit des estimations de travail. AWS Le WQF est inclus avec

AWS Schema Conversion Tool (AWS SCT). Il analyse les schémas de base de données et les objets de code, le code d'application, les dépendances et les caractéristiques de performance, et fournit des rapports d'évaluation.

B

mauvais bot

Un bot destiné à perturber ou à nuire à des individus ou à des organisations.

BCP

Consultez la section Planification de la continuité des activités.

graphique de comportement

Vue unifiée et interactive des comportements des ressources et des interactions au fil du temps. Vous pouvez utiliser un graphique de comportement avec Amazon Detective pour examiner les tentatives de connexion infructueuses, les appels d'API suspects et les actions similaires. Pour plus d'informations, veuillez consulter Data in a behavior graph dans la documentation Detective.

système de poids fort

Système qui stocke d'abord l'octet le plus significatif. Voir aussi endianité.

classification binaire

Processus qui prédit un résultat binaire (l'une des deux classes possibles). Par exemple, votre modèle de machine learning peut avoir besoin de prévoir des problèmes tels que « Cet e-mail est-il du spam ou non ? » ou « Ce produit est-il un livre ou une voiture ? ».

filtre de Bloom

Structure de données probabiliste et efficace en termes de mémoire qui est utilisée pour tester si un élément fait partie d'un ensemble.

déploiement bleu/vert

Stratégie de déploiement dans laquelle vous créez deux environnements distincts mais identiques. Vous exécutez la version actuelle de l'application dans un environnement (bleu) et la nouvelle version de l'application dans l'autre environnement (vert). Cette stratégie vous permet de revenir rapidement en arrière avec un impact minimal.

bot

Application logicielle qui exécute des tâches automatisées sur Internet et simule l'activité ou l'interaction humaine. Certains robots sont utiles ou bénéfiques, comme les robots d'exploration Web qui indexent des informations sur Internet. D'autres robots, appelés « bots malveillants », sont destinés à perturber ou à nuire à des individus ou à des organisations.

botnet

Réseaux de robots infectés par des logiciels malveillants et contrôlés par une seule entité, connue sous le nom d'herder ou d'opérateur de bots. Les botnets sont le mécanisme le plus connu pour faire évoluer les bots et leur impact.

branche

Zone contenue d'un référentiel de code. La première branche créée dans un référentiel est la branche principale. Vous pouvez créer une branche à partir d'une branche existante, puis développer des fonctionnalités ou corriger des bogues dans la nouvelle branche. Une branche que vous créez pour générer une fonctionnalité est communément appelée branche de fonctionnalités. Lorsque la fonctionnalité est prête à être publiée, vous fusionnez à nouveau la branche de fonctionnalités dans la branche principale. Pour plus d'informations, consultez À propos des branches (GitHub documentation).

accès par brise-vitre

Dans des circonstances exceptionnelles et par le biais d'un processus approuvé, c'est un moyen rapide pour un utilisateur d'accéder à un accès auquel Compte AWS il n'est généralement pas autorisé. Pour plus d'informations, consultez l'indicateur Implementation break-glass procedures dans le guide Well-Architected AWS .

stratégie existante (brownfield)

L'infrastructure existante de votre environnement. Lorsque vous adoptez une stratégie existante pour une architecture système, vous concevez l'architecture en fonction des contraintes des systèmes et de l'infrastructure actuels. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

cache de tampon

Zone de mémoire dans laquelle sont stockées les données les plus fréquemment consultées.

capacité métier

Ce que fait une entreprise pour générer de la valeur (par exemple, les ventes, le service client ou le marketing). Les architectures de microservices et les décisions de développement

peuvent être dictées par les capacités métier. Pour plus d'informations, veuillez consulter la section Organisation en fonction des capacités métier du livre blanc Exécution de microservices conteneurisés sur AWS.

planification de la continuité des activités (BCP)

Plan qui tient compte de l'impact potentiel d'un événement perturbateur, tel qu'une migration à grande échelle, sur les opérations, et qui permet à une entreprise de reprendre ses activités rapidement.

C

CAF

Voir le cadre d'adoption du AWS cloud.

déploiement de Canary

Diffusion lente et progressive d'une version pour les utilisateurs finaux. Lorsque vous êtes sûr, vous déployez la nouvelle version et remplacez la version actuelle dans son intégralité.

CCo E

Voir le Centre d'excellence du cloud.

CDC

Voir capture des données de modification.

capture des données de modification (CDC)

Processus de suivi des modifications apportées à une source de données, telle qu'une table de base de données, et d'enregistrement des métadonnées relatives à ces modifications. Vous pouvez utiliser la CDC à diverses fins, telles que l'audit ou la réplication des modifications dans un système cible afin de maintenir la synchronisation.

ingénierie du chaos

Introduire intentionnellement des défaillances ou des événements perturbateurs pour tester la résilience d'un système. Vous pouvez utiliser AWS Fault Injection Service (AWS FIS) pour effectuer des expériences qui stressent vos AWS charges de travail et évaluer leur réponse.

CI/CD

Découvrez l'intégration continue et la livraison continue.

classification

Processus de catégorisation qui permet de générer des prédictions. Les modèles de ML pour les problèmes de classification prédisent une valeur discrète. Les valeurs discrètes se distinguent toujours les unes des autres. Par exemple, un modèle peut avoir besoin d'évaluer la présence ou non d'une voiture sur une image.

chiffrement côté client

Chiffrement des données localement, avant que la cible ne les Service AWS reçoive.

Centre d'excellence du cloud (CCoE)

Une équipe multidisciplinaire qui dirige les efforts d'adoption du cloud au sein d'une organisation, notamment en développant les bonnes pratiques en matière de cloud, en mobilisant des ressources, en établissant des délais de migration et en guidant l'organisation dans le cadre de transformations à grande échelle. Pour plus d'informations, consultez les CCoarticles électroniques du blog sur la stratégie AWS Cloud d'entreprise.

cloud computing

Technologie cloud généralement utilisée pour le stockage de données à distance et la gestion des appareils IoT. Le cloud computing est généralement associé à la technologie informatique de pointe.

modèle d'exploitation du cloud

Dans une organisation informatique, modèle d'exploitation utilisé pour créer, faire évoluer et optimiser un ou plusieurs environnements cloud. Pour plus d'informations, consultez la section Création de votre modèle d'exploitation cloud.

étapes d'adoption du cloud

Les quatre phases que les entreprises traversent généralement lorsqu'elles migrent vers AWS Cloud :

- Projet : exécution de quelques projets liés au cloud à des fins de preuve de concept et d'apprentissage
- Base : réaliser des investissements fondamentaux pour accélérer votre adoption du cloud (par exemple, créer une zone de landing zone, définir un CCo E, établir un modèle opérationnel)
- Migration : migration d'applications individuelles
- Réinvention : optimisation des produits et services et innovation dans le cloud

Ces étapes ont été définies par Stephen Orban dans le billet de blog The Journey Toward Cloud-First & the Stages of Adoption publié sur le blog AWS Cloud Enterprise Strategy. Pour plus d'informations sur leur lien avec la stratégie de AWS migration, consultez le guide de préparation à la migration.

CMDB

Voir base de données de gestion de configuration.

référentiel de code

Emplacement où le code source et d'autres ressources, comme la documentation, les exemples et les scripts, sont stockés et mis à jour par le biais de processus de contrôle de version. Les référentiels cloud courants incluent GitHub ouBitbucket Cloud. Chaque version du code est appelée branche. Dans une structure de microservice, chaque référentiel est consacré à une seule fonctionnalité. Un seul pipeline CI/CD peut utiliser plusieurs référentiels.

cache passif

Cache tampon vide, mal rempli ou contenant des données obsolètes ou non pertinentes. Cela affecte les performances, car l'instance de base de données doit lire à partir de la mémoire principale ou du disque, ce qui est plus lent que la lecture à partir du cache tampon.

données gelées

Données rarement consultées et généralement historiques. Lorsque vous interrogez ce type de données, les requêtes lentes sont généralement acceptables. Le transfert de ces données vers des niveaux ou classes de stockage moins performants et moins coûteux peut réduire les coûts.

vision par ordinateur (CV)

Domaine de l'IA qui utilise l'apprentissage automatique pour analyser et extraire des informations à partir de formats visuels tels que des images numériques et des vidéos. Par exemple, Amazon SageMaker AI fournit des algorithmes de traitement d'image pour les CV.

dérive de configuration

Pour une charge de travail, une modification de configuration par rapport à l'état attendu. Cela peut entraîner une non-conformité de la charge de travail, et cela est généralement progressif et involontaire.

base de données de gestion des configurations (CMDB)

Référentiel qui stocke et gère les informations relatives à une base de données et à son environnement informatique, y compris les composants matériels et logiciels ainsi que leurs

configurations. Vous utilisez généralement les données d'une CMDB lors de la phase de découverte et d'analyse du portefeuille de la migration.

pack de conformité

Ensemble de AWS Config règles et d'actions correctives que vous pouvez assembler pour personnaliser vos contrôles de conformité et de sécurité. Vous pouvez déployer un pack de conformité en tant qu'entité unique dans une région Compte AWS et, ou au sein d'une organisation, à l'aide d'un modèle YAML. Pour plus d'informations, consultez la section Packs de conformité dans la AWS Config documentation.

intégration continue et livraison continue (CI/CD)

Processus d'automatisation des étapes de source, de construction, de test, de préparation et de production du processus de publication du logiciel. CI/CD is commonly described as a pipeline. CI/CDpeut vous aider à automatiser les processus, à améliorer la productivité, à améliorer la qualité du code et à accélérer les livraisons. Pour plus d'informations, veuillez consulter Avantages de la livraison continue. CD peut également signifier déploiement continu. Pour plus d'informations, veuillez consulter Livraison continue et déploiement continu.

CV

Voir vision par ordinateur.

D

données au repos

Données stationnaires dans votre réseau, telles que les données stockées.

classification des données

Processus permettant d'identifier et de catégoriser les données de votre réseau en fonction de leur sévérité et de leur sensibilité. Il s'agit d'un élément essentiel de toute stratégie de gestion des risques de cybersécurité, car il vous aide à déterminer les contrôles de protection et de conservation appropriés pour les données. La classification des données est une composante du pilier de sécurité du AWS Well-Architected Framework. Pour plus d'informations, veuillez consulter Classification des données.

dérive des données

Une variation significative entre les données de production et les données utilisées pour entraîner un modèle ML, ou une modification significative des données d'entrée au fil du temps. La dérive

des données peut réduire la qualité, la précision et l'équité globales des prédictions des modèles ML.

données en transit

Données qui circulent activement sur votre réseau, par exemple entre les ressources du réseau.

maillage de données

Un cadre architectural qui fournit une propriété des données distribuée et décentralisée avec une gestion et une gouvernance centralisées.

minimisation des données

Le principe de collecte et de traitement des seules données strictement nécessaires. La pratique de la minimisation des données AWS Cloud peut réduire les risques liés à la confidentialité, les coûts et l'empreinte carbone de vos analyses.

périmètre de données

Ensemble de garde-fous préventifs dans votre AWS environnement qui permettent de garantir que seules les identités fiables accèdent aux ressources fiables des réseaux attendus. Pour plus d'informations, voir Création d'un périmètre de données sur AWS.

prétraitement des données

Pour transformer les données brutes en un format facile à analyser par votre modèle de ML. Le prétraitement des données peut impliquer la suppression de certaines colonnes ou lignes et le traitement des valeurs manquantes, incohérentes ou en double.

provenance des données

Le processus de suivi de l'origine et de l'historique des données tout au long de leur cycle de vie, par exemple la manière dont les données ont été générées, transmises et stockées.

sujet des données

Personne dont les données sont collectées et traitées.

entrepôt des données

Un système de gestion des données qui prend en charge les informations commerciales, telles que les analyses. Les entrepôts de données contiennent généralement de grandes quantités de données historiques et sont généralement utilisés pour les requêtes et les analyses.

langage de définition de base de données (DDL)

Instructions ou commandes permettant de créer ou de modifier la structure des tables et des objets dans une base de données.

langage de manipulation de base de données (DML)

Instructions ou commandes permettant de modifier (insérer, mettre à jour et supprimer) des informations dans une base de données.

DDL

Voir langage de définition de base de données.

ensemble profond

Sert à combiner plusieurs modèles de deep learning à des fins de prédiction. Vous pouvez utiliser des ensembles profonds pour obtenir une prévision plus précise ou pour estimer l'incertitude des prédictions.

deep learning

Un sous-champ de ML qui utilise plusieurs couches de réseaux neuronaux artificiels pour identifier le mappage entre les données d'entrée et les variables cibles d'intérêt.

defense-in-depth

Approche de la sécurité de l'information dans laquelle une série de mécanismes et de contrôles de sécurité sont judicieusement répartis sur l'ensemble d'un réseau informatique afin de protéger la confidentialité, l'intégrité et la disponibilité du réseau et des données qu'il contient. Lorsque vous adoptez cette stratégie AWS, vous ajoutez plusieurs contrôles à différentes couches de la AWS Organizations structure afin de sécuriser les ressources. Par exemple, une defense-in-depth approche peut combiner l'authentification multifactorielle, la segmentation du réseau et le chiffrement.

administrateur délégué

Dans AWS Organizations, un service compatible peut enregistrer un compte AWS membre pour administrer les comptes de l'organisation et gérer les autorisations pour ce service. Ce compte est appelé administrateur délégué pour ce service. Pour plus d'informations et une liste des services compatibles, veuillez consulter la rubrique Services qui fonctionnent avec AWS Organizations dans la documentation AWS Organizations .

déploiement

Processus de mise à disposition d'une application, de nouvelles fonctionnalités ou de corrections de code dans l'environnement cible. Le déploiement implique la mise en œuvre de modifications dans une base de code, puis la génération et l'exécution de cette base de code dans les environnements de l'application.

environnement de développement

Voir environnement.

contrôle de détection

Contrôle de sécurité conçu pour détecter, journaliser et alerter après la survenue d'un événement. Ces contrôles constituent une deuxième ligne de défense et vous alertent en cas d'événements de sécurité qui ont contourné les contrôles préventifs en place. Pour plus d'informations, veuillez consulter la rubrique Contrôles de détection dans Implementing security controls on AWS.

cartographie de la chaîne de valeur du développement (DVSM)

Processus utilisé pour identifier et hiérarchiser les contraintes qui nuisent à la rapidité et à la qualité du cycle de vie du développement logiciel. DVSM étend le processus de cartographie de la chaîne de valeur initialement conçu pour les pratiques de production allégée. Il met l'accent sur les étapes et les équipes nécessaires pour créer et transférer de la valeur tout au long du processus de développement logiciel.

jumeau numérique

Représentation virtuelle d'un système réel, tel qu'un bâtiment, une usine, un équipement industriel ou une ligne de production. Les jumeaux numériques prennent en charge la maintenance prédictive, la surveillance à distance et l'optimisation de la production.

tableau des dimensions

Dans un schéma en étoile, table plus petite contenant les attributs de données relatifs aux données quantitatives d'une table de faits. Les attributs des tables de dimensions sont généralement des champs de texte ou des nombres discrets qui se comportent comme du texte. Ces attributs sont couramment utilisés pour la contrainte des requêtes, le filtrage et l'étiquetage des ensembles de résultats.

catastrophe

Un événement qui empêche une charge de travail ou un système d'atteindre ses objectifs commerciaux sur son site de déploiement principal. Ces événements peuvent être des

catastrophes naturelles, des défaillances techniques ou le résultat d'actions humaines, telles qu'une mauvaise configuration involontaire ou une attaque de logiciel malveillant.

reprise après sinistre (DR)

La stratégie et le processus que vous utilisez pour minimiser les temps d'arrêt et les pertes de données causés par un sinistre. Pour plus d'informations, consultez Disaster Recovery of Workloads on AWS : Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Voir langage de manipulation de base de données.

conception axée sur le domaine

Approche visant à développer un système logiciel complexe en connectant ses composants à des domaines évolutifs, ou objectifs métier essentiels, que sert chaque composant. Ce concept a été introduit par Eric Evans dans son ouvrage Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston : Addison-Wesley Professional, 2003). Pour plus d'informations sur l'utilisation du design piloté par domaine avec le modèle de figuier étrangleur, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

DR

Voir reprise après sinistre.

détection de dérive

Suivi des écarts par rapport à une configuration de référence. Par exemple, vous pouvez l'utiliser AWS CloudFormation pour détecter la dérive des ressources du système ou AWS Control Tower pour détecter les modifications de votre zone d'atterrissage susceptibles d'affecter le respect des exigences de gouvernance.

DVSM

Voir la cartographie de la chaîne de valeur du développement.

E

EDA

Voir analyse exploratoire des données.

EDI

Voir échange de données informatisé.

informatique de périphérie

Technologie qui augmente la puissance de calcul des appareils intelligents en périphérie d'un réseau IoT. Comparé au cloud computing, l'informatique de pointe peut réduire la latence des communications et améliorer le temps de réponse.

échange de données informatisé (EDI)

L'échange automatique de documents commerciaux entre les organisations. Pour plus d'informations, voir Qu'est-ce que l'échange de données informatisé ?

chiffrement

Processus informatique qui transforme des données en texte clair, lisibles par l'homme, en texte chiffré.

clé de chiffrement

Chaîne cryptographique de bits aléatoires générée par un algorithme cryptographique. La longueur des clés peut varier, et chaque clé est conçue pour être imprévisible et unique.

endianisme

Ordre selon lequel les octets sont stockés dans la mémoire de l'ordinateur. Les systèmes de poids fort stockent d'abord l'octet le plus significatif. Les systèmes de poids faible stockent d'abord l'octet le moins significatif.

point de terminaison

Voir point de terminaison de service.

service de point de terminaison

Service que vous pouvez héberger sur un cloud privé virtuel (VPC) pour le partager avec d'autres utilisateurs. Vous pouvez créer un service de point de terminaison avec AWS PrivateLink et accorder des autorisations à d'autres Comptes AWS ou à AWS Identity and Access Management (IAM) principaux. Ces comptes ou principaux peuvent se connecter à votre service de point de terminaison de manière privée en créant des points de terminaison d'un VPC d'interface. Pour plus d'informations, veuillez consulter Création d'un service de point de terminaison dans la documentation Amazon Virtual Private Cloud (Amazon VPC).

planification des ressources d'entreprise (ERP)

Système qui automatise et gère les principaux processus métier (tels que la comptabilité, le MES et la gestion de projet) pour une entreprise.

chiffrement d'enveloppe

Processus de chiffrement d'une clé de chiffrement à l'aide d'une autre clé de chiffrement. Pour plus d'informations, consultez la section Chiffrement des enveloppes dans la documentation AWS Key Management Service (AWS KMS).

environment

Instance d'une application en cours d'exécution. Les types d'environnement les plus courants dans le cloud computing sont les suivants :

- Environnement de développement : instance d'une application en cours d'exécution à laquelle seule l'équipe principale chargée de la maintenance de l'application peut accéder. Les environnements de développement sont utilisés pour tester les modifications avant de les promouvoir dans les environnements supérieurs. Ce type d'environnement est parfois appelé environnement de test.
- Environnements inférieurs : tous les environnements de développement d'une application, tels que ceux utilisés pour les générations et les tests initiaux.
- Environnement de production : instance d'une application en cours d'exécution à laquelle les utilisateurs finaux peuvent accéder. Dans un pipeline CI/CD, l'environnement de production est le dernier environnement de déploiement.
- Environnements supérieurs : tous les environnements accessibles aux utilisateurs autres que l'équipe de développement principale. Ils peuvent inclure un environnement de production, des environnements de préproduction et des environnements pour les tests d'acceptation par les utilisateurs.

épopée

Dans les méthodologies agiles, catégories fonctionnelles qui aident à organiser et à prioriser votre travail. Les épopées fournissent une description détaillée des exigences et des tâches d'implémentation. Par exemple, les points forts de la AWS CAF en matière de sécurité incluent la gestion des identités et des accès, les contrôles de détection, la sécurité des infrastructures, la protection des données et la réponse aux incidents. Pour plus d'informations sur les épopées dans la stratégie de migration AWS , veuillez consulter le guide d'implémentation du programme.

ERP

Voir Planification des ressources d'entreprise.

analyse exploratoire des données (EDA)

Processus d'analyse d'un jeu de données pour comprendre ses principales caractéristiques. Vous collectez ou agrégez des données, puis vous effectuez des enquêtes initiales pour trouver des modèles, détecter des anomalies et vérifier les hypothèses. L'EDA est réalisée en calculant des statistiques récapitulatives et en créant des visualisations de données.

F

tableau des faits

La table centrale dans un schéma en étoile. Il stocke des données quantitatives sur les opérations commerciales. Généralement, une table de faits contient deux types de colonnes : celles qui contiennent des mesures et celles qui contiennent une clé étrangère pour une table de dimensions.

échouer rapidement

Une philosophie qui utilise des tests fréquents et progressifs pour réduire le cycle de vie du développement. C'est un élément essentiel d'une approche agile.

limite d'isolation des défauts

Dans le AWS Cloud, une limite telle qu'une zone de disponibilité Région AWS, un plan de contrôle ou un plan de données qui limite l'effet d'une panne et contribue à améliorer la résilience des charges de travail. Pour plus d'informations, consultez la section Limites d'isolation des AWS pannes.

branche de fonctionnalités

Voir succursale.

fonctionnalités

Les données d'entrée que vous utilisez pour faire une prédiction. Par exemple, dans un contexte de fabrication, les fonctionnalités peuvent être des images capturées périodiquement à partir de la ligne de fabrication.

importance des fonctionnalités

Le niveau d'importance d'une fonctionnalité pour les prédictions d'un modèle. Il s'exprime généralement sous la forme d'un score numérique qui peut être calculé à l'aide de différentes techniques, telles que la méthode Shapley Additive Explanations (SHAP) et les gradients intégrés. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec AWS.

transformation de fonctionnalité

Optimiser les données pour le processus de ML, notamment en enrichissant les données avec des sources supplémentaires, en mettant à l'échelle les valeurs ou en extrayant plusieurs ensembles d'informations à partir d'un seul champ de données. Cela permet au modèle de ML de tirer parti des données. Par exemple, si vous décomposez la date « 2021-05-27 00:15:37 » en « 2021 », « mai », « jeudi » et « 15 », vous pouvez aider l'algorithme d'apprentissage à apprendre des modèles nuancés associés à différents composants de données.

invitation en quelques coups

Fournir à un LLM un petit nombre d'exemples illustrant la tâche et le résultat souhaité avant de lui demander d'effectuer une tâche similaire. Cette technique est une application de l'apprentissage contextuel, dans le cadre de laquelle les modèles apprennent à partir d'exemples (prises de vue) intégrés dans des instructions. Les instructions en quelques étapes peuvent être efficaces pour les tâches qui nécessitent un formatage, un raisonnement ou des connaissances de domaine spécifiques. Voir également l'invite Zero-Shot.

FGAC

Découvrez le contrôle d'accès détaillé.

contrôle d'accès détaillé (FGAC)

Utilisation de plusieurs conditions pour autoriser ou refuser une demande d'accès.

migration instantanée (flash-cut)

Méthode de migration de base de données qui utilise la réplication continue des données par le biais de la capture des données de modification afin de migrer les données dans les plus brefs délais, au lieu d'utiliser une approche progressive. L'objectif est de réduire au maximum les temps d'arrêt.

FM

Voir le modèle de fondation.

modèle de fondation (FM)

Un vaste réseau neuronal d'apprentissage profond qui s'est entraîné sur d'énormes ensembles de données généralisées et non étiquetées. FMs sont capables d'effectuer une grande variété de tâches générales, telles que comprendre le langage, générer du texte et des images et converser en langage naturel. Pour plus d'informations, voir Que sont les modèles de base ?

G

IA générative

Sous-ensemble de modèles d'IA qui ont été entraînés sur de grandes quantités de données et qui peuvent utiliser une simple invite textuelle pour créer de nouveaux contenus et artefacts, tels que des images, des vidéos, du texte et du son. Pour plus d'informations, consultez Qu'est-ce que l'IA générative.

blocage géographique

Voir les restrictions géographiques.

restrictions géographiques (blocage géographique)

Sur Amazon CloudFront, option permettant d'empêcher les utilisateurs de certains pays d'accéder aux distributions de contenu. Vous pouvez utiliser une liste d'autorisation ou une liste de blocage pour spécifier les pays approuvés et interdits. Pour plus d'informations, consultez la section Restreindre la distribution géographique de votre contenu dans la CloudFront documentation.

Flux de travail Gitflow

Approche dans laquelle les environnements inférieurs et supérieurs utilisent différentes branches dans un référentiel de code source. Le flux de travail Gitflow est considéré comme existant, et le flux de travail basé sur les troncs est l'approche moderne préférée.

image dorée

Un instantané d'un système ou d'un logiciel utilisé comme modèle pour déployer de nouvelles instances de ce système ou logiciel. Par exemple, dans le secteur de la fabrication, une image dorée peut être utilisée pour fournir des logiciels sur plusieurs appareils et contribue à améliorer la vitesse, l'évolutivité et la productivité des opérations de fabrication des appareils.

stratégie inédite

L'absence d'infrastructures existantes dans un nouvel environnement. Lorsque vous adoptez une stratégie inédite pour une architecture système, vous pouvez sélectionner toutes les nouvelles technologies sans restriction de compatibilité avec l'infrastructure existante, également appelée brownfield. Si vous étendez l'infrastructure existante, vous pouvez combiner des politiques brownfield (existantes) et greenfield (inédites).

barrière de protection

Règle de haut niveau qui permet de régir les ressources, les politiques et la conformité au sein des unités organisationnelles (OUs). Les barrières de protection préventives appliquent des politiques pour garantir l'alignement sur les normes de conformité. Elles sont mises en œuvre à l'aide de politiques de contrôle des services et de limites des autorisations IAM. Les barrières de protection de détection détectent les violations des politiques et les problèmes de conformité, et génèrent des alertes pour y remédier. Ils sont implémentés à l'aide d'Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, d'Amazon Inspector et de AWS Lambda contrôles personnalisés.

H

HA

Découvrez la haute disponibilité.

migration de base de données hétérogène

Migration de votre base de données source vers une base de données cible qui utilise un moteur de base de données différent (par exemple, Oracle vers Amazon Aurora). La migration hétérogène fait généralement partie d'un effort de réarchitecture, et la conversion du schéma peut s'avérer une tâche complexe. AWS propose AWS SCT qui facilite les conversions de schémas.

haute disponibilité (HA)

Capacité d'une charge de travail à fonctionner en continu, sans intervention, en cas de difficultés ou de catastrophes. Les systèmes HA sont conçus pour basculer automatiquement, fournir constamment des performances de haute qualité et gérer différentes charges et défaillances avec un impact minimal sur les performances.

modernisation des historiens

Approche utilisée pour moderniser et mettre à niveau les systèmes de technologie opérationnelle (OT) afin de mieux répondre aux besoins de l'industrie manufacturière. Un historien est un type de base de données utilisé pour collecter et stocker des données provenant de diverses sources dans une usine.

données de rétention

Partie de données historiques étiquetées qui n'est pas divulguée dans un ensemble de données utilisé pour entraîner un modèle d'apprentissage automatique. Vous pouvez utiliser les données de blocage pour évaluer les performances du modèle en comparant les prévisions du modèle aux données de blocage.

migration de base de données homogène

Migration de votre base de données source vers une base de données cible qui partage le même moteur de base de données (par exemple, Microsoft SQL Server vers Amazon RDS for SQL Server). La migration homogène s'inscrit généralement dans le cadre d'un effort de réhébergement ou de replateforme. Vous pouvez utiliser les utilitaires de base de données natifs pour migrer le schéma.

données chaudes

Données fréquemment consultées, telles que les données en temps réel ou les données translationnelles récentes. Ces données nécessitent généralement un niveau ou une classe de stockage à hautes performances pour fournir des réponses rapides aux requêtes.

correctif

Solution d'urgence à un problème critique dans un environnement de production. En raison de son urgence, un correctif est généralement créé en dehors du flux de travail de DevOps publication habituel.

période de soins intensifs

Immédiatement après le basculement, période pendant laquelle une équipe de migration gère et surveille les applications migrées dans le cloud afin de résoudre les problèmes éventuels. En règle générale, cette période dure de 1 à 4 jours. À la fin de la période de soins intensifs, l'équipe de migration transfère généralement la responsabilité des applications à l'équipe des opérations cloud.

I

IaC

Considérez l'infrastructure comme un code.

politique basée sur l’identité

Politique attachée à un ou plusieurs principaux IAM qui définit leurs autorisations au sein de l' AWS Cloud environnement.

application inactive

Application dont l'utilisation moyenne du processeur et de la mémoire se situe entre 5 et 20 % sur une période de 90 jours. Dans un projet de migration, il est courant de retirer ces applications ou de les retenir sur site.

IIo T

Voir Internet industriel des objets.

infrastructure immuable

Modèle qui déploie une nouvelle infrastructure pour les charges de travail de production au lieu de mettre à jour, d'appliquer des correctifs ou de modifier l'infrastructure existante. Les infrastructures immuables sont intrinsèquement plus cohérentes, fiables et prévisibles que les infrastructures mutables. Pour plus d'informations, consultez les meilleures pratiques de déploiement à l'aide d'une infrastructure immuable dans le AWS Well-Architected Framework.

VPC entrant (d'entrée)

Dans une architecture AWS multi-comptes, un VPC qui accepte, inspecte et achemine les connexions réseau depuis l'extérieur d'une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

migration incrémentielle

Stratégie de basculement dans le cadre de laquelle vous migrez votre application par petites parties au lieu d'effectuer un basculement complet unique. Par exemple, il se peut que vous ne transfériez que quelques microservices ou utilisateurs vers le nouveau système dans un premier temps. Après avoir vérifié que tout fonctionne correctement, vous pouvez transférer

progressivement des microservices ou des utilisateurs supplémentaires jusqu'à ce que vous puissiez mettre hors service votre système hérité. Cette stratégie réduit les risques associés aux migrations de grande ampleur.

Industry 4.0

Terme introduit par Klaus Schwab en 2016 pour désigner la modernisation des processus de fabrication grâce aux avancées en matière de connectivité, de données en temps réel, d'automatisation, d'analyse et d'IA/ML.

infrastructure

Ensemble des ressources et des actifs contenus dans l'environnement d'une application.

infrastructure en tant que code (IaC)

Processus de mise en service et de gestion de l'infrastructure d'une application via un ensemble de fichiers de configuration. IaC est conçue pour vous aider à centraliser la gestion de l'infrastructure, à normaliser les ressources et à mettre à l'échelle rapidement afin que les nouveaux environnements soient reproductibles, fiables et cohérents.

Internet industriel des objets (IIoT)

L'utilisation de capteurs et d'appareils connectés à Internet dans les secteurs industriels tels que la fabrication, l'énergie, l'automobile, les soins de santé, les sciences de la vie et l'agriculture. Pour plus d'informations, voir Élaboration d'une stratégie de transformation numérique de l'Internet des objets (IIoT) industriel.

VPC d'inspection

Dans une architecture AWS multi-comptes, un VPC centralisé qui gère les inspections du trafic réseau VPCs entre (identique ou Régions AWS différent), Internet et les réseaux locaux. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

Internet des objets (IoT)

Réseau d'objets physiques connectés dotés de capteurs ou de processeurs intégrés qui communiquent avec d'autres appareils et systèmes via Internet ou via un réseau de communication local. Pour plus d'informations, veuillez consulter la section Qu'est-ce que l'IoT ?.

interprétabilité

Caractéristique d'un modèle de machine learning qui décrit dans quelle mesure un être humain peut comprendre comment les prédictions du modèle dépendent de ses entrées. Pour plus d'informations, voir Interprétabilité du modèle d'apprentissage automatique avec AWS.

IoT

Voir Internet des objets.

Bibliothèque d'informations informatiques (ITIL)

Ensemble de bonnes pratiques pour proposer des services informatiques et les aligner sur les exigences métier. L'ITIL constitue la base de l'ITSM.

gestion des services informatiques (ITSM)

Activités associées à la conception, à la mise en œuvre, à la gestion et à la prise en charge de services informatiques d'une organisation. Pour plus d'informations sur l'intégration des opérations cloud aux outils ITSM, veuillez consulter le guide d'intégration des opérations.

ITIL

Consultez la bibliothèque d'informations informatiques.

ITSM

Voir Gestion des services informatiques.

L

contrôle d'accès basé sur des étiquettes (LBAC)

Une implémentation du contrôle d'accès obligatoire (MAC) dans laquelle une valeur d'étiquette de sécurité est explicitement attribuée aux utilisateurs et aux données elles-mêmes. L'intersection entre l'étiquette de sécurité utilisateur et l'étiquette de sécurité des données détermine les lignes et les colonnes visibles par l'utilisateur.

zone de destination

Une zone d'atterrissage est un AWS environnement multi-comptes bien conçu, évolutif et sécurisé. Il s'agit d'un point de départ à partir duquel vos entreprises peuvent rapidement lancer et déployer des charges de travail et des applications en toute confiance dans leur environnement de sécurité et d'infrastructure. Pour plus d'informations sur les zones de destination, veuillez consulter Setting up a secure and scalable multi-account AWS environment.

grand modèle de langage (LLM)

Un modèle d'intelligence artificielle basé sur le deep learning qui est préentraîné sur une grande quantité de données. Un LLM peut effectuer plusieurs tâches, telles que répondre à des questions, résumer des documents, traduire du texte dans d'autres langues et compléter des phrases. Pour plus d'informations, voir Que sont LLMs.

migration de grande envergure

Migration de 300 serveurs ou plus.

LBAC

Voir contrôle d'accès basé sur des étiquettes.

principe de moindre privilège

Bonne pratique de sécurité qui consiste à accorder les autorisations minimales nécessaires à l'exécution d'une tâche. Pour plus d'informations, veuillez consulter la rubrique Accorder les autorisations de moindre privilège dans la documentation IAM.

lift and shift

Voir 7 Rs.

système de poids faible

Système qui stocke d'abord l'octet le moins significatif. Voir aussi endianité.

LLM

Voir le grand modèle de langage.

environnements inférieurs

Voir environnement.

M

machine learning (ML)

Type d'intelligence artificielle qui utilise des algorithmes et des techniques pour la reconnaissance et l'apprentissage de modèles. Le ML analyse et apprend à partir de données enregistrées, telles que les données de l'Internet des objets (IoT), pour générer un modèle statistique basé sur des modèles. Pour plus d'informations, veuillez consulter Machine Learning.

branche principale

Voir succursale.

malware

Logiciel conçu pour compromettre la sécurité ou la confidentialité de l'ordinateur. Les logiciels malveillants peuvent perturber les systèmes informatiques, divulguer des informations sensibles ou obtenir un accès non autorisé. Parmi les malwares, on peut citer les virus, les vers, les rançongiciels, les chevaux de Troie, les logiciels espions et les enregistreurs de frappe.

services gérés

Services AWS pour lequel AWS fonctionnent la couche d'infrastructure, le système d'exploitation et les plateformes, et vous accédez aux points de terminaison pour stocker et récupérer des données. Amazon Simple Storage Service (Amazon S3) et Amazon DynamoDB sont des exemples de services gérés. Ils sont également connus sous le nom de services abstraits.

système d'exécution de la fabrication (MES)

Un système logiciel pour le suivi, la surveillance, la documentation et le contrôle des processus de production qui convertissent les matières premières en produits finis dans l'atelier.

MAP

Voir Migration Acceleration Program.

mécanisme

Processus complet au cours duquel vous créez un outil, favorisez son adoption, puis inspectez les résultats afin de procéder aux ajustements nécessaires. Un mécanisme est un cycle qui se renforce et s'améliore au fur et à mesure de son fonctionnement. Pour plus d'informations, voir Création de mécanismes dans le cadre AWS Well-Architected.

compte membre

Tous, à l' Comptes AWS exception du compte de gestion, qui font partie d'une organisation dans AWS Organizations. Un compte ne peut être membre que d'une seule organisation à la fois.

MAILLES

Voir le système d'exécution de la fabrication.

Transport télémétrique en file d'attente de messages (MQTT)

Protocole de communication léger machine-to-machine (M2M), basé sur le modèle de publication/d'abonnement, pour les appareils IoT aux ressources limitées.

microservice

Un petit service indépendant qui communique via un réseau bien défini APIs et qui est généralement détenu par de petites équipes autonomes. Par exemple, un système d'assurance peut inclure des microservices qui mappent à des capacités métier, telles que les ventes ou le marketing, ou à des sous-domaines, tels que les achats, les réclamations ou l'analytique. Les avantages des microservices incluent l'agilité, la flexibilité de la mise à l'échelle, la facilité de déploiement, la réutilisation du code et la résilience. Pour plus d'informations, consultez la section Intégration de microservices à l'aide de services AWS sans serveur.

architecture de microservices

Approche de création d'une application avec des composants indépendants qui exécutent chaque processus d'application en tant que microservice. Ces microservices communiquent via une interface bien définie en utilisant Lightweight. APIs Chaque microservice de cette architecture peut être mis à jour, déployé et mis à l'échelle pour répondre à la demande de fonctions spécifiques d'une application. Pour plus d'informations, consultez la section Implémentation de microservices sur AWS.

Programme d'accélération des migrations (MAP)

Un AWS programme qui fournit un support de conseil, des formations et des services pour aider les entreprises à établir une base opérationnelle solide pour passer au cloud, et pour aider à compenser le coût initial des migrations. MAP inclut une méthodologie de migration pour exécuter les migrations héritées de manière méthodique, ainsi qu'un ensemble d'outils pour automatiser et accélérer les scénarios de migration courants.

migration à grande échelle

Processus consistant à transférer la majeure partie du portefeuille d'applications vers le cloud par vagues, un plus grand nombre d'applications étant déplacées plus rapidement à chaque vague. Cette phase utilise les bonnes pratiques et les enseignements tirés des phases précédentes pour implémenter une usine de migration d'équipes, d'outils et de processus en vue de rationaliser la migration des charges de travail grâce à l'automatisation et à la livraison agile. Il s'agit de la troisième phase de la stratégie de migration AWS.

usine de migration

Équipes interfonctionnelles qui rationalisent la migration des charges de travail grâce à des approches automatisées et agiles. Les équipes de Migration Factory comprennent généralement des responsables des opérations, des analystes commerciaux et des propriétaires, des ingénieurs de migration, des développeurs et DevOps des professionnels travaillant dans le cadre de sprints.

Entre 20 et 50 % du portefeuille d'applications d'entreprise est constitué de modèles répétés qui peuvent être optimisés par une approche d'usine. Pour plus d'informations, veuillez consulter la rubrique discussion of migration factories et le guide Cloud Migration Factory dans cet ensemble de contenus.

métadonnées de migration

Informations relatives à l'application et au serveur nécessaires pour finaliser la migration. Chaque modèle de migration nécessite un ensemble de métadonnées de migration différent. Les exemples de métadonnées de migration incluent le sous-réseau cible, le groupe de sécurité et le AWS compte.

modèle de migration

Tâche de migration reproductible qui détaille la stratégie de migration, la destination de la migration et l'application ou le service de migration utilisé. Exemple : réorganisez la migration vers Amazon EC2 avec le service de migration AWS d'applications.

Évaluation du portefeuille de migration (MPA)

Outil en ligne qui fournit des informations pour valider l'analyse de rentabilisation en faveur de la migration vers le. AWS Cloud La MPA propose une évaluation détaillée du portefeuille (dimensionnement approprié des serveurs, tarification, comparaison du coût total de possession, analyse des coûts de migration), ainsi que la planification de la migration (analyse et collecte des données d'applications, regroupement des applications, priorisation des migrations et planification des vagues). L'outil MPA (connexion requise) est disponible gratuitement pour tous les AWS consultants et consultants APN Partner.

Évaluation de la préparation à la migration (MRA)

Processus qui consiste à obtenir des informations sur l'état de préparation d'une organisation au cloud, à identifier les forces et les faiblesses et à élaborer un plan d'action pour combler les lacunes identifiées, à l'aide du AWS CAF. Pour plus d'informations, veuillez consulter le guide de préparation à la migration. La MRA est la première phase de la stratégie de migration AWS.

stratégie de migration

L'approche utilisée pour migrer une charge de travail vers le AWS Cloud. Pour plus d'informations, reportez-vous aux 7 R de ce glossaire et à Mobiliser votre organisation pour accélérer les migrations à grande échelle.

ML

Voir apprentissage automatique.

modernisation

Transformation d'une application obsolète (héritée ou monolithique) et de son infrastructure en un système agile, élastique et hautement disponible dans le cloud afin de réduire les coûts, de gagner en efficacité et de tirer parti des innovations. Pour plus d'informations, consultez la section Stratégie de modernisation des applications dans le AWS Cloud.

évaluation de la préparation à la modernisation

Évaluation qui permet de déterminer si les applications d'une organisation sont prêtes à être modernisées, d'identifier les avantages, les risques et les dépendances, et qui détermine dans quelle mesure l'organisation peut prendre en charge l'état futur de ces applications. Le résultat de l'évaluation est un plan de l'architecture cible, une feuille de route détaillant les phases de développement et les étapes du processus de modernisation, ainsi qu'un plan d'action pour combler les lacunes identifiées. Pour plus d'informations, consultez la section Évaluation de l'état de préparation à la modernisation des applications dans le AWS Cloud.

applications monolithiques (monolithes)

Applications qui s'exécutent en tant que service unique avec des processus étroitement couplés. Les applications monolithiques ont plusieurs inconvénients. Si une fonctionnalité de l'application connaît un pic de demande, l'architecture entière doit être mise à l'échelle. L'ajout ou l'amélioration des fonctionnalités d'une application monolithique devient également plus complexe lorsque la base de code s'élargit. Pour résoudre ces problèmes, vous pouvez utiliser une architecture de microservices. Pour plus d'informations, veuillez consulter Decomposing monoliths into microservices.

MPA

Voir Évaluation du portefeuille de migration.

MQTT

Voir Message Queuing Telemetry Transport.

classification multi-classes

Processus qui permet de générer des prédictions pour plusieurs classes (prédiction d'un résultat parmi plus de deux). Par exemple, un modèle de ML peut demander « Ce produit est-il un livre, une voiture ou un téléphone ? » ou « Quelle catégorie de produits intéresse le plus ce client ? ».

infrastructure mutable

Modèle qui met à jour et modifie l'infrastructure existante pour les charges de travail de production. Pour améliorer la cohérence, la fiabilité et la prévisibilité, le AWS Well-Architected Framework recommande l'utilisation d'une infrastructure immuable comme meilleure pratique.

O

OAC

Voir Contrôle d'accès à l'origine.

OAI

Voir l'identité d'accès à l'origine.

OCM

Voir gestion du changement organisationnel.

migration hors ligne

Méthode de migration dans laquelle la charge de travail source est supprimée au cours du processus de migration. Cette méthode implique un temps d'arrêt prolongé et est généralement utilisée pour de petites charges de travail non critiques.

OI

Voir Intégration des opérations.

OLA

Voir l'accord au niveau opérationnel.

migration en ligne

Méthode de migration dans laquelle la charge de travail source est copiée sur le système cible sans être mise hors ligne. Les applications connectées à la charge de travail peuvent continuer à fonctionner pendant la migration. Cette méthode implique un temps d'arrêt nul ou minimal et est généralement utilisée pour les charges de travail de production critiques.

OPC-UA

Voir Open Process Communications - Architecture unifiée.

Communications par processus ouvert - Architecture unifiée (OPC-UA)

Un protocole de communication machine-to-machine (M2M) pour l'automatisation industrielle. L'OPC-UA fournit une norme d'interopérabilité avec des schémas de cryptage, d'authentification et d'autorisation des données.

accord au niveau opérationnel (OLA)

Accord qui précise ce que les groupes informatiques fonctionnels s'engagent à fournir les uns aux autres, afin de prendre en charge un contrat de niveau de service (SLA).

examen de l'état de préparation opérationnelle (ORR)

Une liste de questions et de bonnes pratiques associées qui vous aident à comprendre, évaluer, prévenir ou réduire l'ampleur des incidents et des défaillances possibles. Pour plus d'informations, voir Operational Readiness Reviews (ORR) dans le AWS Well-Architected Framework.

technologie opérationnelle (OT)

Systèmes matériels et logiciels qui fonctionnent avec l'environnement physique pour contrôler les opérations, les équipements et les infrastructures industriels. Dans le secteur manufacturier, l'intégration des systèmes OT et des technologies de l'information (IT) est au cœur des transformations de l'industrie 4.0.

intégration des opérations (OI)

Processus de modernisation des opérations dans le cloud, qui implique la planification de la préparation, l'automatisation et l'intégration. Pour en savoir plus, veuillez consulter le guide d'intégration des opérations.

journal de suivi d'organisation

Un parcours créé par AWS CloudTrail qui enregistre tous les événements pour tous les membres Comptes AWS d'une organisation dans AWS Organizations. Ce journal de suivi est créé dans chaque Compte AWS qui fait partie de l'organisation et suit l'activité de chaque compte. Pour plus d'informations, consultez la section Création d'un suivi pour une organisation dans la CloudTrail documentation.

gestion du changement organisationnel (OCM)

Cadre pour gérer les transformations métier majeures et perturbatrices du point de vue des personnes, de la culture et du leadership. L'OCM aide les organisations à se préparer et à effectuer la transition vers de nouveaux systèmes et de nouvelles politiques en accélérant

l'adoption des changements, en abordant les problèmes de transition et en favorisant des changements culturels et organisationnels. Dans la stratégie de AWS migration, ce cadre est appelé accélération du personnel, en raison de la rapidité du changement requise dans les projets d'adoption du cloud. Pour plus d'informations, veuillez consulter le guide OCM.

contrôle d'accès d'origine (OAC)

Dans CloudFront, une option améliorée pour restreindre l'accès afin de sécuriser votre contenu Amazon Simple Storage Service (Amazon S3). L'OAC prend en charge tous les compartiments S3 dans leur ensemble Régions AWS, le chiffrement côté serveur avec AWS KMS (SSE-KMS) et les requêtes dynamiques PUT adressées au compartiment S3. DELETE

identité d'accès d'origine (OAI)

Dans CloudFront, une option permettant de restreindre l'accès afin de sécuriser votre contenu Amazon S3. Lorsque vous utilisez OAI, il CloudFront crée un principal auprès duquel Amazon S3 peut s'authentifier. Les principaux authentifiés ne peuvent accéder au contenu d'un compartiment S3 que par le biais d'une distribution spécifique CloudFront . Voir également OAC, qui fournit un contrôle d'accès plus précis et amélioré.

ORR

Voir l'examen de l'état de préparation opérationnelle.

DE

Voir technologie opérationnelle.

VPC sortant (de sortie)

Dans une architecture AWS multi-comptes, un VPC qui gère les connexions réseau initiées depuis une application. L'architecture AWS de référence de sécurité recommande de configurer votre compte réseau avec les fonctions entrantes, sortantes et d'inspection VPCs afin de protéger l'interface bidirectionnelle entre votre application et l'Internet en général.

P

limite des autorisations

Politique de gestion IAM attachée aux principaux IAM pour définir les autorisations maximales que peut avoir l'utilisateur ou le rôle. Pour plus d'informations, veuillez consulter la rubrique Limites des autorisations dans la documentation IAM.

informations personnelles identifiables (PII)

Informations qui, lorsqu'elles sont consultées directement ou associées à d'autres données connexes, peuvent être utilisées pour déduire raisonnablement l'identité d'une personne. Les exemples d'informations personnelles incluent les noms, les adresses et les informations de contact.

PII

Voir les informations personnelles identifiables.

manuel stratégique

Ensemble d'étapes prédéfinies qui capturent le travail associé aux migrations, comme la fourniture de fonctions d'opérations de base dans le cloud. Un manuel stratégique peut revêtir la forme de scripts, de runbooks automatisés ou d'un résumé des processus ou des étapes nécessaires au fonctionnement de votre environnement modernisé.

PLC

Voir contrôleur logique programmable.

PLM

Consultez la section Gestion du cycle de vie des produits.

politique

Objet capable de définir les autorisations (voir la politique basée sur l'identité), de spécifier les conditions d'accès (voir la politique basée sur les ressources) ou de définir les autorisations maximales pour tous les comptes d'une organisation dans AWS Organizations (voir la politique de contrôle des services).

persistance polyglotte

Choix indépendant de la technologie de stockage de données d'un microservice en fonction des modèles d'accès aux données et d'autres exigences. Si vos microservices utilisent la même technologie de stockage de données, ils peuvent rencontrer des difficultés d'implémentation ou présenter des performances médiocres. Les microservices sont plus faciles à mettre en œuvre, atteignent de meilleures performances, ainsi qu'une meilleure capacité de mise à l'échelle s'ils utilisent l'entrepôt de données le mieux adapté à leurs besoins. Pour plus d'informations, veuillez consulter Enabling data persistence in microservices.

évaluation du portefeuille

Processus de découverte, d'analyse et de priorisation du portefeuille d'applications afin de planifier la migration. Pour plus d'informations, veuillez consulter Evaluating migration readiness.

predicate

Une condition de requête qui renvoie `true` ou`false`, généralement située dans une `WHERE` clause.

prédicat pushdown

Technique d'optimisation des requêtes de base de données qui filtre les données de la requête avant le transfert. Cela réduit la quantité de données qui doivent être extraites et traitées à partir de la base de données relationnelle et améliore les performances des requêtes.

contrôle préventif

Contrôle de sécurité conçu pour empêcher qu'un événement ne se produise. Ces contrôles constituent une première ligne de défense pour empêcher tout accès non autorisé ou toute modification indésirable de votre réseau. Pour plus d'informations, veuillez consulter Preventative controls dans Implementing security controls on AWS.

principal

Entité capable d'effectuer AWS des actions et d'accéder à des ressources. Cette entité est généralement un utilisateur root pour un Compte AWS rôle IAM ou un utilisateur. Pour plus d'informations, veuillez consulter la rubrique Principal dans Termes et concepts relatifs aux rôles, dans la documentation IAM.

confidentialité dès la conception

Une approche d'ingénierie système qui prend en compte la confidentialité tout au long du processus de développement.

zones hébergées privées

Conteneur contenant des informations sur la manière dont vous souhaitez qu'Amazon Route 53 réponde aux requêtes DNS pour un domaine et ses sous-domaines au sein d'un ou de plusieurs VPCs domaines. Pour plus d'informations, veuillez consulter Working with private hosted zones dans la documentation Route 53.

contrôle proactif

Contrôle de sécurité conçu pour empêcher le déploiement de ressources non conformes. Ces contrôles analysent les ressources avant qu'elles ne soient provisionnées. Si la ressource n'est

pas conforme au contrôle, elle n'est pas provisionnée. Pour plus d'informations, consultez le guide de référence sur les contrôles dans la AWS Control Tower documentation et consultez la section Contrôles proactifs dans Implémentation des contrôles de sécurité sur AWS.

gestion du cycle de vie des produits (PLM)

Gestion des données et des processus d'un produit tout au long de son cycle de vie, depuis la conception, le développement et le lancement, en passant par la croissance et la maturité, jusqu'au déclin et au retrait.

environnement de production

Voir environnement.

contrôleur logique programmable (PLC)

Dans le secteur manufacturier, un ordinateur hautement fiable et adaptable qui surveille les machines et automatise les processus de fabrication.

chaînage rapide

Utiliser le résultat d'une invite LLM comme entrée pour l'invite suivante afin de générer de meilleures réponses. Cette technique est utilisée pour décomposer une tâche complexe en sous-tâches ou pour affiner ou développer de manière itérative une réponse préliminaire. Cela permet d'améliorer la précision et la pertinence des réponses d'un modèle et permet d'obtenir des résultats plus précis et personnalisés.

pseudonymisation

Processus de remplacement des identifiants personnels dans un ensemble de données par des valeurs fictives. La pseudonymisation peut contribuer à protéger la vie privée. Les données pseudonymisées sont toujours considérées comme des données personnelles.

publish/subscribe (pub/sub)

Modèle qui permet des communications asynchrones entre les microservices afin d'améliorer l'évolutivité et la réactivité. Par exemple, dans un MES basé sur des microservices, un microservice peut publier des messages d'événements sur un canal auquel d'autres microservices peuvent s'abonner. Le système peut ajouter de nouveaux microservices sans modifier le service de publication.

Q

plan de requête

Série d'étapes, telles que des instructions, utilisées pour accéder aux données d'un système de base de données relationnelle SQL.

régression du plan de requêtes

Le cas où un optimiseur de service de base de données choisit un plan moins optimal qu'avant une modification donnée de l'environnement de base de données. Cela peut être dû à des changements en termes de statistiques, de contraintes, de paramètres d'environnement, de liaisons de paramètres de requêtes et de mises à jour du moteur de base de données.

R

Matrice RACI

Voir responsable, responsable, consulté, informé (RACI).

CHIFFON

Voir Retrieval Augmented Generation.

rançongiciel

Logiciel malveillant conçu pour bloquer l'accès à un système informatique ou à des données jusqu'à ce qu'un paiement soit effectué.

Matrice RASCI

Voir responsable, responsable, consulté, informé (RACI).

RCAC

Voir contrôle d'accès aux lignes et aux colonnes.

réplica en lecture

Copie d'une base de données utilisée en lecture seule. Vous pouvez acheminer les requêtes vers le réplica de lecture pour réduire la charge sur votre base de données principale.

réarchitecte

Voir 7 Rs.

objectif de point de récupération (RPO)

Durée maximale acceptable depuis le dernier point de récupération des données. Il détermine ce qui est considéré comme étant une perte de données acceptable entre le dernier point de reprise et l'interruption du service.

objectif de temps de récupération (RTO)

Le délai maximum acceptable entre l'interruption du service et le rétablissement du service.

refactoriser

Voir 7 Rs.

Région

Un ensemble de AWS ressources dans une zone géographique. Chacun Région AWS est isolé et indépendant des autres pour garantir tolérance aux pannes, stabilité et résilience. Pour plus d'informations, voir Spécifier ce que Régions AWS votre compte peut utiliser.

régression

Technique de ML qui prédit une valeur numérique. Par exemple, pour résoudre le problème « Quel sera le prix de vente de cette maison ? », un modèle de ML pourrait utiliser un modèle de régression linéaire pour prédire le prix de vente d'une maison sur la base de faits connus à son sujet (par exemple, la superficie en mètres carrés).

réhéberger

Voir 7 Rs.

version

Dans un processus de déploiement, action visant à promouvoir les modifications apportées à un environnement de production.

déplacer

Voir 7 Rs.

replateforme

Voir 7 Rs.

rachat

Voir 7 Rs.

résilience

La capacité d'une application à résister aux perturbations ou à s'en remettre. La haute disponibilité et la reprise après sinistre sont des considérations courantes lors de la planification de la résilience dans le AWS Cloud. Pour plus d'informations, consultez la section AWS Cloud Résilience.

politique basée sur les ressources

Politique attachée à une ressource, comme un compartiment Amazon S3, un point de terminaison ou une clé de chiffrement. Ce type de politique précise les principaux auxquels l'accès est autorisé, les actions prises en charge et toutes les autres conditions qui doivent être remplies.

matrice responsable, redevable, consulté et informé (RACI)

Une matrice qui définit les rôles et les responsabilités de toutes les parties impliquées dans les activités de migration et les opérations cloud. Le nom de la matrice est dérivé des types de responsabilité définis dans la matrice : responsable (R), responsable (A), consulté (C) et informé (I). Le type de support (S) est facultatif. Si vous incluez le support, la matrice est appelée matrice RASCI, et si vous l'excluez, elle est appelée matrice RACI.

contrôle réactif

Contrôle de sécurité conçu pour permettre de remédier aux événements indésirables ou aux écarts par rapport à votre référence de sécurité. Pour plus d'informations, veuillez consulter la rubrique Responsive controls dans Implementing security controls on AWS.

retain

Voir 7 Rs.

se retirer

Voir 7 Rs.

Génération augmentée de récupération (RAG)

Technologie d'IA générative dans laquelle un LLM fait référence à une source de données faisant autorité qui se trouve en dehors de ses sources de données de formation avant de générer une réponse. Par exemple, un modèle RAG peut effectuer une recherche sémantique dans la base de connaissances ou dans les données personnalisées d'une organisation. Pour plus d'informations, voir Qu'est-ce que RAG ?

rotation

Processus de mise à jour périodique d'un secret pour empêcher un attaquant d'accéder aux informations d'identification.

contrôle d'accès aux lignes et aux colonnes (RCAC)

Utilisation d'expressions SQL simples et flexibles dotées de règles d'accès définies. Le RCAC comprend des autorisations de ligne et des masques de colonnes.

RPO

Voir l'objectif du point de récupération.

RTO

Voir l'objectif relatif au temps de rétablissement.

runbook

Ensemble de procédures manuelles ou automatisées nécessaires à l'exécution d'une tâche spécifique. Elles visent généralement à rationaliser les opérations ou les procédures répétitives présentant des taux d'erreur élevés.

S

SAML 2.0

Un standard ouvert utilisé par de nombreux fournisseurs d'identité (IdPs). Cette fonctionnalité permet l'authentification unique fédérée (SSO), afin que les utilisateurs puissent se connecter AWS Management Console ou appeler les opérations de l' AWS API sans que vous ayez à créer un utilisateur dans IAM pour tous les membres de votre organisation. Pour plus d'informations sur la fédération SAML 2.0, veuillez consulter À propos de la fédération SAML 2.0 dans la documentation IAM.

SCADA

Voir Contrôle de supervision et acquisition de données.

SCP

Voir la politique de contrôle des services.

secret

Dans AWS Secrets Manager des informations confidentielles ou restreintes, telles qu'un mot de passe ou des informations d'identification utilisateur, que vous stockez sous forme cryptée. Il comprend la valeur secrète et ses métadonnées. La valeur secrète peut être binaire, une chaîne unique ou plusieurs chaînes. Pour plus d'informations, voir Que contient le secret d'un Secrets Manager ? dans la documentation de Secrets Manager.

sécurité dès la conception

Une approche d'ingénierie système qui prend en compte la sécurité tout au long du processus de développement.

contrôle de sécurité

Barrière de protection technique ou administrative qui empêche, détecte ou réduit la capacité d'un assaillant d'exploiter une vulnérabilité de sécurité. Il existe quatre principaux types de contrôles de sécurité : préventifs, détectifs, réactifs et proactifs.

renforcement de la sécurité

Processus qui consiste à réduire la surface d'attaque pour la rendre plus résistante aux attaques. Cela peut inclure des actions telles que la suppression de ressources qui ne sont plus requises, la mise en œuvre des bonnes pratiques de sécurité consistant à accorder le moindre privilège ou la désactivation de fonctionnalités inutiles dans les fichiers de configuration.

système de gestion des informations et des événements de sécurité (SIEM)

Outils et services qui associent les systèmes de gestion des informations de sécurité (SIM) et de gestion des événements de sécurité (SEM). Un système SIEM collecte, surveille et analyse les données provenant de serveurs, de réseaux, d'appareils et d'autres sources afin de détecter les menaces et les failles de sécurité, mais aussi de générer des alertes.

automatisation des réponses de sécurité

Action prédéfinie et programmée conçue pour répondre automatiquement à un événement de sécurité ou y remédier. Ces automatisations servent de contrôles de sécurité détectifs ou réactifs qui vous aident à mettre en œuvre les meilleures pratiques AWS de sécurité. Parmi les actions de réponse automatique, citons la modification d'un groupe de sécurité VPC, l'application de correctifs à une EC2 instance Amazon ou la rotation des informations d'identification.

chiffrement côté serveur

Chiffrement des données à destination, par celui Service AWS qui les reçoit.

Politique de contrôle des services (SCP)

Politique qui fournit un contrôle centralisé des autorisations pour tous les comptes d'une organisation dans AWS Organizations. SCPs définissez des garde-fous ou des limites aux actions qu'un administrateur peut déléguer à des utilisateurs ou à des rôles. Vous pouvez les utiliser SCPs comme listes d'autorisation ou de refus pour spécifier les services ou les actions autorisés ou interdits. Pour plus d'informations, consultez la section Politiques de contrôle des services dans la AWS Organizations documentation.

point de terminaison du service

URL du point d'entrée pour un Service AWS. Pour vous connecter par programmation au service cible, vous pouvez utiliser un point de terminaison. Pour plus d'informations, veuillez consulter la rubrique Service AWS endpoints dans Références générales AWS.

contrat de niveau de service (SLA)

Accord qui précise ce qu'une équipe informatique promet de fournir à ses clients, comme le temps de disponibilité et les performances des services.

indicateur de niveau de service (SLI)

Mesure d'un aspect des performances d'un service, tel que son taux d'erreur, sa disponibilité ou son débit.

objectif de niveau de service (SLO)

Mesure cible qui représente l'état d'un service, tel que mesuré par un indicateur de niveau de service.

modèle de responsabilité partagée

Un modèle décrivant la responsabilité que vous partagez en matière AWS de sécurité et de conformité dans le cloud. AWS est responsable de la sécurité du cloud, alors que vous êtes responsable de la sécurité dans le cloud. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée.

SIEM

Consultez les informations de sécurité et le système de gestion des événements.

point de défaillance unique (SPOF)

Défaillance d'un seul composant critique d'une application susceptible de perturber le système.

SLA

Voir le contrat de niveau de service.

SLI

Voir l'indicateur de niveau de service.

SLO

Voir l'objectif de niveau de service.

split-and-seed modèle

Modèle permettant de mettre à l'échelle et d'accélérer les projets de modernisation. Au fur et à mesure que les nouvelles fonctionnalités et les nouvelles versions de produits sont définies, l'équipe principale se divise pour créer des équipes de produit. Cela permet de mettre à l'échelle les capacités et les services de votre organisation, d'améliorer la productivité des développeurs et de favoriser une innovation rapide. Pour plus d'informations, consultez la section Approche progressive de la modernisation des applications dans le. AWS Cloud

SPOF

Voir point de défaillance unique.

schéma en étoile

Structure organisationnelle de base de données qui utilise une grande table de faits pour stocker les données transactionnelles ou mesurées et utilise une ou plusieurs tables dimensionnelles plus petites pour stocker les attributs des données. Cette structure est conçue pour être utilisée dans un entrepôt de données ou à des fins de business intelligence.

modèle de figuier étrangleur

Approche de modernisation des systèmes monolithiques en réécrivant et en remplaçant progressivement les fonctionnalités du système jusqu'à ce que le système hérité puisse être mis hors service. Ce modèle utilise l'analogie d'un figuier de vigne qui se développe dans un arbre existant et qui finit par supplanter son hôte. Le schéma a été présenté par Martin Fowler comme un moyen de gérer les risques lors de la réécriture de systèmes monolithiques. Pour obtenir un exemple d'application de ce modèle, veuillez consulter Modernizing legacy Microsoft ASP.NET (ASMX) web services incrementally by using containers and Amazon API Gateway.

sous-réseau

Plage d'adresses IP dans votre VPC. Un sous-réseau doit se trouver dans une seule zone de disponibilité.

contrôle de supervision et acquisition de données (SCADA)

Dans le secteur manufacturier, un système qui utilise du matériel et des logiciels pour surveiller les actifs physiques et les opérations de production.

chiffrement symétrique

Algorithme de chiffrement qui utilise la même clé pour chiffrer et déchiffrer les données.

tests synthétiques

Tester un système de manière à simuler les interactions des utilisateurs afin de détecter les problèmes potentiels ou de surveiller les performances. Vous pouvez utiliser Amazon CloudWatch Synthetics pour créer ces tests.

invite du système

Technique permettant de fournir un contexte, des instructions ou des directives à un LLM afin d'orienter son comportement. Les instructions du système aident à définir le contexte et à établir des règles pour les interactions avec les utilisateurs.

T

balises

Des paires clé-valeur qui agissent comme des métadonnées pour organiser vos AWS ressources. Les balises peuvent vous aider à gérer, identifier, organiser, rechercher et filtrer des ressources. Pour plus d'informations, veuillez consulter la rubrique Balisage de vos AWS ressources.

variable cible

La valeur que vous essayez de prédire dans le cadre du ML supervisé. Elle est également qualifiée de variable de résultat. Par exemple, dans un environnement de fabrication, la variable cible peut être un défaut du produit.

liste de tâches

Outil utilisé pour suivre les progrès dans un runbook. Liste de tâches qui contient une vue d'ensemble du runbook et une liste des tâches générales à effectuer. Pour chaque tâche générale, elle inclut le temps estimé nécessaire, le propriétaire et l'avancement.

environnement de test

Voir environnement.

entraînement

Pour fournir des données à partir desquelles votre modèle de ML peut apprendre. Les données d'entraînement doivent contenir la bonne réponse. L'algorithme d'apprentissage identifie des modèles dans les données d'entraînement, qui mettent en correspondance les attributs des données d'entrée avec la cible (la réponse que vous souhaitez prédire). Il fournit un modèle de ML qui capture ces modèles. Vous pouvez alors utiliser le modèle de ML pour obtenir des prédictions sur de nouvelles données pour lesquelles vous ne connaissez pas la cible.

passerelle de transit

Un hub de transit réseau que vous pouvez utiliser pour interconnecter vos réseaux VPCs et ceux sur site. Pour plus d'informations, voir Qu'est-ce qu'une passerelle de transit dans la AWS Transit Gateway documentation.

flux de travail basé sur jonction

Approche selon laquelle les développeurs génèrent et testent des fonctionnalités localement dans une branche de fonctionnalités, puis fusionnent ces modifications dans la branche principale. La branche principale est ensuite intégrée aux environnements de développement, de préproduction et de production, de manière séquentielle.

accès sécurisé

Accorder des autorisations à un service que vous spécifiez pour effectuer des tâches au sein de votre organisation AWS Organizations et dans ses comptes en votre nom. Le service de confiance crée un rôle lié au service dans chaque compte, lorsque ce rôle est nécessaire, pour effectuer des tâches de gestion à votre place. Pour plus d'informations, consultez la section Utilisation AWS Organizations avec d'autres AWS services dans la AWS Organizations documentation.

réglage

Pour modifier certains aspects de votre processus d'entraînement afin d'améliorer la précision du modèle de ML. Par exemple, vous pouvez entraîner le modèle de ML en générant un ensemble d'étiquetage, en ajoutant des étiquettes, puis en répétant ces étapes plusieurs fois avec différents paramètres pour optimiser le modèle.

équipe de deux pizzas

Une petite DevOps équipe que vous pouvez nourrir avec deux pizzas. Une équipe de deux pizzas garantit les meilleures opportunités de collaboration possible dans le développement de logiciels.

U

incertitude

Un concept qui fait référence à des informations imprécises, incomplètes ou inconnues susceptibles de compromettre la fiabilité des modèles de ML prédictifs. Il existe deux types d'incertitude : l'incertitude épistémique est causée par des données limitées et incomplètes, alors que l'incertitude aléatoire est causée par le bruit et le caractère aléatoire inhérents aux données. Pour plus d'informations, veuillez consulter le guide Quantifying uncertainty in deep learning systems.

tâches indifférenciées

Également connu sous le nom de « levage de charges lourdes », ce travail est nécessaire pour créer et exploiter une application, mais qui n'apporte pas de valeur directe à l'utilisateur final ni d'avantage concurrentiel. Les exemples de tâches indifférenciées incluent l'approvisionnement, la maintenance et la planification des capacités.

environnements supérieurs

Voir environnement.

V

mise à vide

Opération de maintenance de base de données qui implique un nettoyage après des mises à jour incrémentielles afin de récupérer de l'espace de stockage et d'améliorer les performances.

contrôle de version

Processus et outils permettant de suivre les modifications, telles que les modifications apportées au code source dans un référentiel.

Appairage de VPC

Une connexion entre deux VPCs qui vous permet d'acheminer le trafic en utilisant des adresses IP privées. Pour plus d'informations, veuillez consulter la rubrique Qu'est-ce que l'appairage de VPC ? dans la documentation Amazon VPC.

vulnérabilités

Défaut logiciel ou matériel qui compromet la sécurité du système.

W

cache actif

Cache tampon qui contient les données actuelles et pertinentes fréquemment consultées. L'instance de base de données peut lire à partir du cache tampon, ce qui est plus rapide que la lecture à partir de la mémoire principale ou du disque.

données chaudes

Données rarement consultées. Lorsque vous interrogez ce type de données, des requêtes modérément lentes sont généralement acceptables.

fonction de fenêtre

Fonction SQL qui effectue un calcul sur un groupe de lignes liées d'une manière ou d'une autre à l'enregistrement en cours. Les fonctions de fenêtre sont utiles pour traiter des tâches, telles que le calcul d'une moyenne mobile ou l'accès à la valeur des lignes en fonction de la position relative de la ligne en cours.

charge de travail

Ensemble de ressources et de code qui fournit une valeur métier, par exemple une application destinée au client ou un processus de backend.

flux de travail

Groupes fonctionnels d'un projet de migration chargés d'un ensemble de tâches spécifique. Chaque flux de travail est indépendant, mais prend en charge les autres flux de travail du projet. Par exemple, le flux de travail du portefeuille est chargé de prioriser les applications, de planifier les vagues et de collecter les métadonnées de migration. Le flux de travail du portefeuille fournit ces actifs au flux de travail de migration, qui migre ensuite les serveurs et les applications.

VER

Voir écrire une fois, lire plusieurs.

WQF

Voir le cadre AWS de qualification de la charge de travail.

écrire une fois, lire plusieurs (WORM)

Modèle de stockage qui écrit les données une seule fois et empêche leur suppression ou leur modification. Les utilisateurs autorisés peuvent lire les données autant de fois que nécessaire,

mais ils ne peuvent pas les modifier. Cette infrastructure de stockage de données est considérée comme immuable.

Z

exploit Zero-Day

Une attaque, généralement un logiciel malveillant, qui tire parti d'une vulnérabilité de type « jour zéro ».

vulnérabilité « jour zéro »

Une faille ou une vulnérabilité non atténuée dans un système de production. Les acteurs malveillants peuvent utiliser ce type de vulnérabilité pour attaquer le système. Les développeurs prennent souvent conscience de la vulnérabilité à la suite de l'attaque.

invite Zero-Shot

Fournir à un LLM des instructions pour effectuer une tâche, mais aucun exemple (plans) pouvant aider à la guider. Le LLM doit utiliser ses connaissances pré-entraînées pour gérer la tâche. L'efficacité de l'invite zéro dépend de la complexité de la tâche et de la qualité de l'invite. Voir également les instructions en quelques clics.

application zombie

Application dont l'utilisation moyenne du processeur et de la mémoire est inférieure à 5 %. Dans un projet de migration, il est courant de retirer ces applications.

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.