Implementierung einer Strategie zur Bot-Kontrolle am AWS

AWS Präskriptive Leitlinien

AWS Präskriptive Leitlinien: Implementierung einer Strategie zur Bot-Kontrolle am AWS

Table of Contents

Implementierung einer Strategie zur Bot-Kontrolle auf AWS

Amazon Web Services (Mitwirkende)

Februar 2024 (Verlauf der Dokumente)

Das Internet, wie wir es kennen, wäre ohne Bots nicht möglich. Bots führen automatisierte Aufgaben über das Internet aus und simulieren menschliche Aktivitäten oder Interaktionen. Sie ermöglichen es Unternehmen, Prozesse und Aufgaben effizienter zu gestalten. Nützliche Bots wie Webcrawler indexieren Informationen im Internet und helfen uns, schnell die relevantesten Informationen für unsere Suchanfragen zu finden. Bots sind ein guter Mechanismus, um das Geschäft zu verbessern und Unternehmen einen Mehrwert zu bieten. Mit der Zeit begannen böswillige Akteure jedoch, Bots als Mittel zu nutzen, um bestehende Systeme und Anwendungen auf neue und kreative Weise zu missbrauchen.

Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung. Botnetze sind Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Von einem zentralen Punkt aus kann der Betreiber jedem Computer in seinem Botnetz befehlen, gleichzeitig eine koordinierte Aktion auszuführen, weshalb Botnetze auch als command-and-control (C2) -Systeme bezeichnet werden.

Die Größe eines Botnetzes kann viele Millionen von Bots betragen. Ein Botnetz hilft dem Betreiber, groß angelegte Aktionen durchzuführen. Da Botnetze weiterhin von einem Fernoperator gesteuert werden, können infizierte Maschinen Updates erhalten und ihr Verhalten spontan ändern. Aus diesem Grund können C2-Systeme den Zugang zu Teilen ihres Botnetzes auf dem Schwarzmarkt vermieten, um einen erheblichen finanziellen Gewinn zu erzielen.

Die Verbreitung von Botnetzen hat weiter zugenommen. Es wird von Experten als das beliebteste Instrument schlechter Schauspieler angesehen. Mirai ist eines der größten Botnetze. Es wurde 2016 gegründet, ist immer noch in Betrieb und hat schätzungsweise bis zu 350.000 Geräte des Internet der Dinge (IoT) infiziert. Dieses Botnetz wurde angepasst und für viele Arten von Aktivitäten verwendet, darunter Distributed-Denial-of-Service-Angriffe (DDoS). In jüngerer Zeit versuchten böswillige Akteure, ihre Aktivitäten weiter zu verschleiern und ihren Datenverkehr zu generieren, indem sie IP-Adressen mithilfe von Proxydiensten für Privatanwender erhielten. Dadurch entsteht ein legitimes, miteinander verbundenes peer-to-peer System, das die Aktivität raffinierter macht und es schwieriger macht, sie zu erkennen und zu bekämpfen.

Dieses Dokument konzentriert sich auf die Bot-Landschaft, ihre Auswirkungen auf Ihre Anwendungen sowie auf die verfügbaren Strategien und Abhilfemaßnahmen. Diese präskriptiven Leitlinien und

die darin enthaltenen Best Practices helfen Ihnen dabei, die verschiedenen Arten von Bot-Angriffen zu verstehen und abzuwehren. Darüber hinaus werden in diesem Leitfaden die Funktionen AWS-Services und Funktionen beschrieben, die eine Strategie zur Abwehr von Bots unterstützen, und wie jede einzelne Strategie Ihnen helfen kann, Ihre Anwendungen zu schützen. Es enthält auch einen Überblick über die Bot-Überwachung und bewährte Methoden zur Optimierung der Lösungskosten.

Bot-Bedrohungen und -Operationen verstehen

Laut Security Today sind mehr als 47% des gesamten Datenverkehrs im Internet auf Bots zurückzuführen. Dazu gehört auch der hilfreiche Teil der Bots, also solche, die sich selbst identifizieren und einen Mehrwert bieten. Etwa 30% des Bot-Traffics sind unbekannte Bots, die bösartige Aktivitäten wie DDo S-Angriffe, Ticket-Scalping, Inventar-Scraping oder Horten ausführen. Das Security Magazine berichtet von einem Anstieg der volumetrischen S-Ereignisse um 300% im ersten Halbjahr 2023 DDo. Dies macht dieses Thema relevanter und macht das Wissen über die verfügbaren präventiven und schützenden Instrumente und Technologien umso wichtiger.

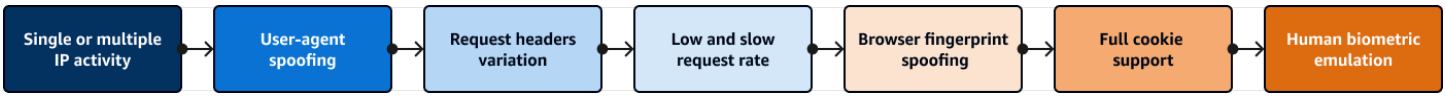
In der folgenden Tabelle werden die verschiedenen Arten von Bot-Aktivitäten und die Auswirkungen, die jede einzelne auf das Unternehmen haben kann, kategorisiert. Dies soll keine umfangreiche Liste sein, sondern eine Zusammenfassung der häufigsten Bot-Aktivitäten. Sie unterstreicht die Bedeutung von Überwachungs- und Minderungskontrollen. Eine umfangreiche Liste von Bot-Bedrohungen finden Sie im Handbuch zu automatisierten Bedrohungen für Anwendungen von OWASP (OWASP-Website).

Art der Bot-Aktivität	Description	Mögliche Auswirkungen
Scraping von Inhalten	Kopieren von urheberrechtlich geschützten Inhalten zur Verwendung durch Websites Dritter	Auswirkungen auf Ihre Suchmaschinenoptimierung aufgrund von Duplizierung von Inhalten, Markenwirkung und Leistungsproblemen, die durch aggressive Scraper verursach t werden
Füllen Sie Ihre Anmeldedaten aus	Testen gestohlener Datenbank en mit Anmeldeinformationen auf Ihrer Website, um Zugriff auf Informationen zu erhalten oder diese zu überprüfen	Probleme für Benutzer, wie Betrug und Kontosperrungen, die zu mehr Support-Anfragen führen und das Markenver trauen verringern
Karten knacken	Testen von Datenbanken mit gestohlenen Kreditkar tendaten zur Validierung oder	Probleme für Benutzer, wie Identitätsdiebstahl und Betrug, und Beschädigung Ihrer Betrugsquote

Art der Bot-Aktivität	Description	Mögliche Auswirkungen
	Ergänzung fehlender Informationen	
Denial of Service	Erhöhen Sie den Traffic auf einer bestimmten Website, um die Reaktion zu verlangsamen oder die Website für legitimen Traffic nicht verfügbar zu machen	Umsatzverlust und Rufschädigung
Erstellung eines Kontos	Einrichtung mehrerer Konten mit dem Zweck des Missbrauchs oder des finanziellen Gewinns	Behindertes Wachstum und verzerrte Marketinganalysen
Skalpieren	Beschaffung von Waren mit begrenzter Verfügbarkeit, häufig Tickets, gegenüber echten Verbrauchern	Umsatzeinbußen und Probleme für die Nutzer, z. B. mangelnder Zugang zu verkauften Waren

Wie funktionieren Botnetze

Die Taktiken, Techniken und Verfahren (TTP) der Botnetzbetreiber haben sich im Laufe der Zeit erheblich weiterentwickelt. Sie mussten mit den von Unternehmen entwickelten Erkennungs- und Abwehrtechnologien Schritt halten. Die folgende Abbildung zeigt diese Entwicklung. Botnets nutzten zunächst einfach IP-Adressen als Betriebsmittel und entwickelten sich schließlich zu einer ausgeklügelten, menschlichen biometrischen Emulation. Diese Raffinesse ist teuer, und nicht alle Botnetze verwenden die fortschrittlichsten Tools. Im Internet gibt es eine Vielzahl von Betreibern, die wahrscheinlich das beste Tool für die jeweilige Aufgabe suchen, um eine gute Investitionsrendite zu erzielen. Ein Ziel der Bot-Abwehr besteht darin, die Botnet-Aktivität zu verteuern, sodass das Ziel nicht mehr lebensfähig ist.



Im Allgemeinen werden Bots als häufig oder gezielt eingestuft:

- Häufige Bots — Diese Bots identifizieren sich selbst und versuchen nicht, Browser zu emulieren. Viele dieser Bots erfüllen nützliche Aufgaben wie das Crawlen von Inhalten, Suchmaschinenoptimierung (SEO) oder Aggregation. Es ist wichtig, zu identifizieren und zu verstehen, welche dieser häufigen Bots auf Ihre Website gelangen und welche Auswirkungen sie auf Ihren Traffic und Ihre Leistung haben.
- Gezielte Bots — Diese Bots versuchen, der Erkennung zu entgehen, indem sie Browser emulieren. Sie verwenden Browsertechnologien, wie z. B. Headless-Browser, oder sie fälschen Browser-Fingerabdrücke. Sie haben die Fähigkeit, Cookies auszuführen JavaScript und zu unterstützen. Ihre Absicht ist nicht immer klar, und der von ihnen generierte Verkehr kann wie normaler Benutzerverkehr aussehen.

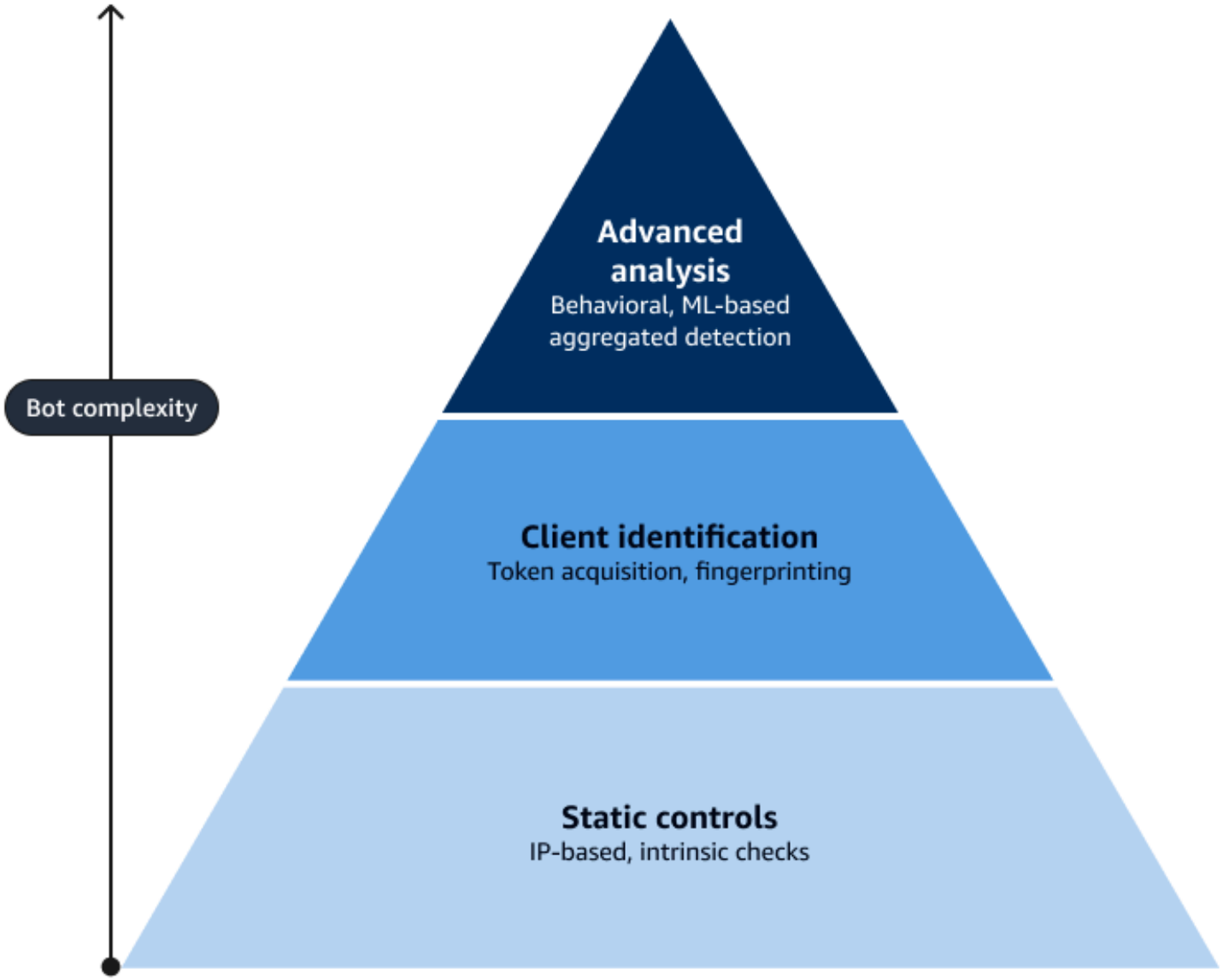
Die fortschrittlichsten und hartnäckigsten zielgerichteten Bots emulieren menschliches Verhalten, indem sie menschenähnliche Mausbewegungen und Klicks auf einer Website erzeugen. Sie sind am ausgefeiltesten und am schwierigsten zu erkennen, aber sie sind auch am teuersten im Betrieb.

Oft kombiniert ein Bediener diese Techniken. Dadurch entsteht ein Spiel der ständigen Verfolgung, bei dem Sie den Schutz- und Minderungsansatz häufig ändern müssen, um sich an die neuesten Techniken des Betreibers anzupassen. Diese Bots gelten als Advanced Persistent Threat (APT). Weitere Informationen finden Sie unter Advanced Persistent Threat im NIST Resource Center.

Techniken zur Bot-Kontrolle

Das Hauptziel der Bot-Abwehr besteht darin, die negativen Auswirkungen automatisierter Bot-Aktivitäten auf die Websites, Dienste und Anwendungen eines Unternehmens zu begrenzen. Die verwendeten Technologien und Techniken hängen von der Art des Datenverkehrs oder der Aktivität ab, gegen die Sie sich schützen möchten. Um dies zu erreichen, ist es wichtig, die Anwendung und ihren Datenverkehr zu verstehen. Weitere Informationen darüber, wo Sie anfangen sollen, finden Sie im Richtlinien für die Überwachung Ihrer Bot-Kontrollstrategie Abschnitt dieses Handbuchs.

Im Allgemeinen lassen sich die Kontrollen, die Lösungen zur Abwehr von Bots bieten, in die folgenden übergeordneten Kategorien einteilen: statisch, Kundenidentifikation und erweiterte Analyse. Die folgende Abbildung zeigt die verschiedenen verfügbaren Techniken und wie sie je nach Komplexität der Bot-Aktivität eingesetzt werden können. Hier wird verdeutlicht, wie die Grundlage oder die umfassendste Abhilfemaßnahme durch den Einsatz statischer Kontrollen, wie z. B. der Listung von Zulassungen und systeminterne Prüfungen, erreicht werden kann. Der kleinste Teil der Bots ist immer der fortschrittlichste, und die Abwehr dieser Bots erfordert fortschrittlichere Technologien und eine Kombination von Kontrollen.



Als Nächstes untersucht dieser Leitfaden jede Kategorie und ihre Techniken. Außerdem werden die Optionen beschrieben, die AWS WAFzur Implementierung dieser Steuerelemente verfügbar sind:

- Statische Steuerelemente für die Verwaltung von Bots
- Kontrollen zur Client-Identifizierung für die Verwaltung von Bots
- Erweiterte Analysefunktionen für die Verwaltung von Bots

Statische Steuerelemente für die Verwaltung von Bots

Um eine Maßnahme zu ergreifen, werten statische Kontrollen statische Informationen aus der HTTP (S) -Anfrage aus, z. B. ihre IP-Adresse oder ihre Header. Diese Kontrollen können nützlich sein bei

bösartigen Bot-Aktivitäten mit geringer Komplexität oder bei erwartetem nutzbringendem Bot-Traffic, der verifiziert und verwaltet werden muss. Zu den statischen Kontrollmethoden gehören: Auflisten von Zulassungen, IP-basierte Kontrollen und interne Prüfungen.

Auflistung zulassen

Bei der Option „Eintrag zulassen“ handelt es sich um ein Steuerelement, das identifizierten, freundlichen Traffic mithilfe vorhandener Kontrollen zur Abwehr von Bots ermöglicht. Es gibt eine Vielzahl von Möglichkeiten, dies zu erreichen. Am einfachsten ist es, eine Regel zu verwenden, die einer Reihe von IP-Adressen oder einer ähnlichen Übereinstimmungsbedingung entspricht. Wenn eine Anforderung mit einer Regel übereinstimmt, die auf eine `Allow` Aktion festgelegt ist, wird sie nicht durch nachfolgende Regeln ausgewertet. In einigen Fällen müssen Sie verhindern, dass nur auf bestimmte Regeln reagiert wird. Mit anderen Worten, Sie müssen die Liste für eine Regel zulassen, aber nicht für alle Regeln. Dies ist ein übliches Szenario für den Umgang mit falsch positiven Ergebnissen bei Regeln. Die Option „Liste zulassen“ wird als Regel mit umfassendem Geltungsbereich betrachtet. Um das Risiko falsch negativer Ergebnisse zu verringern, empfehlen wir, diese Option mit einer anderen detaillierteren Option zu kombinieren, z. B. einem Pfad- oder Header-Abgleich.

IP-basierte Steuerungen

Einzelne IP-Adressblöcke

Ein häufig verwendetes Tool zur Minderung der Auswirkungen von Bots besteht darin, Anfragen von einem einzelnen Anforderer zu begrenzen. Das einfachste Beispiel besteht darin, die Quell-IP-Adresse des Datenverkehrs zu blockieren, wenn die Anfragen böswillig sind oder ein hohes Volumen aufweisen. Dabei werden AWS WAF IP-Set-Übereinstimmungsregeln verwendet, um IP-basierte Blöcke zu implementieren. Diese Regeln stimmen bei IP-Adressen überein und wenden die Aktion `BlockChallenge`, oder `CAPTCHA` an. Sie können anhand des Content Delivery Network (CDN), einer Firewall für Webanwendungen oder Anwendungs- und Dienstprotokolle feststellen, wann zu viele Anfragen von einer IP-Adresse eingehen. In den meisten Fällen ist diese Steuerung jedoch ohne Automatisierung nicht praktikabel.

Die Automatisierung von Blocklisten für IP-Adressen AWS WAF erfolgt üblicherweise mit ratenbasierten Regeln. Weitere Informationen finden Sie unter Ratenbasierte Regeln in diesem Handbuch. Sie können auch die Sicherheitsautomatisierung als Lösung implementieren. AWS WAF Diese Lösung aktualisiert automatisch eine Liste von IP-Adressen, die blockiert werden sollen, und eine AWS WAF Regel lehnt Anfragen ab, die diesen IP-Adressen entsprechen.

Eine Möglichkeit, einen Bot-Angriff zu erkennen, besteht darin, dass sich eine Vielzahl von Anfragen von derselben IP-Adresse auf eine kleine Anzahl von Webseiten konzentriert. Dies deutet darauf hin, dass der Bot Preise verschrottet oder wiederholt versucht, Logins zu starten, die zu einem hohen Prozentsatz fehlschlagen. Sie können Automatisierungen erstellen, die dieses Muster sofort erkennen. Die Automatisierungen blockieren die IP-Adresse, wodurch die Wirksamkeit des Angriffs verringert wird, da er schnell identifiziert und abgewehrt wird. Das Blockieren bestimmter IP-Adressen ist weniger effektiv, wenn ein Angreifer über eine große Sammlung von IP-Adressen verfügt, von denen aus er Angriffe starten kann, oder wenn das Angriffsverhalten schwer zu erkennen und vom normalen Datenverkehr zu trennen ist.

Reputation von IP-Adressen

Ein IP-Reputationsdienst liefert Informationen, anhand derer die Vertrauenswürdigkeit einer IP-Adresse bewertet werden kann. Diese Informationen werden üblicherweise durch die Zusammenfassung von IP-bezogenen Informationen aus vergangenen Aktivitäten anhand dieser IP-Adresse gewonnen. Frühere Aktivitäten geben Aufschluss darüber, wie wahrscheinlich es ist, dass eine IP-Adresse bösartige Anfragen generiert. Die Daten werden zu verwalteten Listen hinzugefügt, die das Verhalten von IP-Adressen verfolgen.

Anonyme IP-Adressen sind ein Spezialfall der Reputation von IP-Adressen. Die Quell-IP-Adresse stammt aus bekannten Quellen leicht zu beschaffender IP-Adressen, wie z. B. cloudbasierten virtuellen Maschinen, oder von Proxys wie bekannten VPN-Anbietern oder Tor-Knoten. Die verwalteten Regelgruppen AWS WAF Amazon IP Reputation List und Anonymous IP List verwenden interne Bedrohungsinformationen von Amazon, um diese IP-Adressen zu identifizieren.

Die von diesen verwalteten Listen bereitgestellten Informationen können Ihnen helfen, auf Aktivitäten zu reagieren, die aus diesen Quellen identifiziert wurden. Auf der Grundlage dieser Informationen können Sie Regeln erstellen, die den Datenverkehr direkt blockieren, oder Regeln, die die Anzahl der Anfragen begrenzen (z. B. ratenbasierte Regeln). Sie können diese Informationen auch verwenden, um die Quelle des Datenverkehrs zu bewerten, indem Sie die Regeln im `COUNT` Modus verwenden. Dabei werden die Übereinstimmungskriterien untersucht und Beschriftungen zugewiesen, anhand derer Sie benutzerdefinierte Regeln erstellen können.

Ratenbasierte Regeln

Ratenbasierte Regeln können für bestimmte Szenarien ein wertvolles Tool sein. Ratenbasierte Regeln sind beispielsweise wirksam, wenn der Bot-Verkehr im Vergleich zu Benutzern mit sensiblen Uniform Resource Identifiers (URIs) ein hohes Volumen erreicht oder wenn das Datenverkehrsvolumen beginnt, den normalen Betrieb zu beeinträchtigen. Durch die

Ratenbegrenzung können Anfragen auf einem überschaubaren Niveau gehalten und der Zugriff eingeschränkt und kontrolliert werden. AWS WAF kann mithilfe einer ratenbasierten Regelanweisung eine Regel zur Ratenbegrenzung in einer Web-Zugriffskontrollliste (Web ACL) implementieren. Ein empfohlener Ansatz bei der Verwendung ratenbasierter Regeln besteht darin, eine pauschale Regel, die die gesamte Site abdeckt, URI-spezifische Regeln und Regeln, die auf IP-Reputationsraten basieren, aufzunehmen. Regeln, die auf der IP-Reputationsrate basieren, kombinieren die Intelligenz der IP-Reputation mit Funktionen zur Ratenbegrenzung.

Eine pauschale Regel, die auf der IP-Reputationsrate basiert, legt für die gesamte Site eine Obergrenze fest, die verhindert, dass unkomplizierte Bots eine Site von einer kleinen Anzahl von aus überfluten. IPs Die Ratenbegrenzung wird vor allem für den Schutz empfohlen, der mit hohen Kosten oder Auswirkungen verbunden ist URIs , wie z. B. Anmeldeseiten oder Seiten zur Kontoerstellung.

Regeln zur Ratenbegrenzung können eine kosteneffiziente erste Schutzebene bieten. Sie können erweiterte Regeln verwenden, um sensible Daten zu schützen. URIs URI-spezifische ratenbasierte Regeln können die Auswirkungen auf kritische Seiten oder solche, die sich auf das Backend auswirken APIs , wie z. B. den Datenbankzugriff, begrenzen. Fortgeschrittene Abhilfemaßnahmen zum Schutz bestimmter Bereiche URIs, auf die weiter unten in diesem Leitfaden eingegangen wird, sind häufig mit zusätzlichen Kosten verbunden, und diese URI-spezifischen ratenbasierten Regeln können Ihnen helfen, die Kosten zu kontrollieren. Weitere Informationen zu häufig empfohlenen ratenbasierten Regeln finden Sie im Sicherheitsblog unter Die drei wichtigsten ratenbasierten Regeln. AWS WAF AWS In manchen Situationen ist es sinnvoll, die Art der Anfrage, die anhand einer ratenbasierten Regel bewertet wird, einzuschränken. Sie können Scopedown-Anweisungen verwenden, um beispielsweise ratenbasierte Regeln auf das geografische Gebiet der Quell-IP-Adresse zu beschränken.

AWS WAF bietet mithilfe von Aggregationsschlüsseln erweiterte Funktionen für ratenbasierte Regeln. Mit dieser Funktion können Sie eine ratenbasierte Regel so konfigurieren, dass sie neben der Quell-IP-Adresse auch verschiedene andere Aggregationsschlüssel und Tastenkombinationen verwendet. Als einzelne Kombination können Sie beispielsweise Anfragen auf der Grundlage einer weitergeleiteten IP-Adresse, der HTTP-Methode und eines Abfragearguments aggregieren. Auf diese Weise können Sie detailliertere Regeln für eine ausgeklügelte Reduzierung des volumetrischen Datenverkehrs konfigurieren.

Intrinsische Prüfungen

Bei intrinsischen Prüfungen handelt es sich um verschiedene Arten interner oder inhärenter Validierungen oder Überprüfungen innerhalb eines Systems oder Prozesses. AWS WAF Führt bei

der Bot-Kontrolle eine systeminterne Prüfung durch, indem überprüft wird, ob die in der Anfrage gesendeten Informationen mit den Systemsignalen übereinstimmen. Es führt beispielsweise umgekehrte DNS-Suchen und andere Systemüberprüfungen durch. Einige automatisierte Anfragen sind erforderlich, z. B. SEO-bezogene Anfragen. Die Option „Eintrag zulassen“ ist eine Möglichkeit, gute, erwartungsgemäße Bots durchzulassen. Aber manchmal emulieren böswillige Bots gute Bots, und es kann schwierig sein, sie voneinander zu trennen. AWS WAF bietet Methoden, um dies mithilfe der verwalteten AWS WAF Bot-Control-Regelgruppe zu erreichen. Die Regeln in dieser Gruppe verifizieren, dass selbst identifizierte Bots auch die sind, für die sie sich ausgeben. AWS WAF überprüft die Details der Anfrage anhand des bekannten Musters dieses Bots und führt außerdem umgekehrte DNS-Suchen und andere objektive Überprüfungen durch.

Kontrollen zur Client-Identifizierung für die Verwaltung von Bots

Wenn der Datenverkehr im Zusammenhang mit Angriffen nicht einfach anhand statischer Attribute erkannt werden kann, muss die Erkennung in der Lage sein, den Client, der die Anfrage stellt, genau zu identifizieren. Ratenbasierte Regeln sind beispielsweise oft effektiver und schwieriger zu umgehen, wenn das Attribut, für das die Ratenbegrenzung gilt, anwendungsspezifisch ist, z. B. ein Cookie oder ein Token. Die Verwendung eines an eine Sitzung gebundenen Cookies verhindert, dass Botnetzbetreiber ähnliche Anforderungsflüsse über viele Bots hinweg duplizieren können.

Die Token-Erfassung wird häufig zur Kundenidentifikation verwendet. Bei der Tokenerfassung sammelt ein JavaScript Code Informationen, um ein Token zu generieren, das serverseitig ausgewertet wird. Die Auswertung kann von der Überprüfung der Ausführung auf dem Client bis hin JavaScript zur Erfassung von Geräteinformationen für Fingerabdrücke reichen. Für die Token-Akquisition ist die Integration eines JavaScript SDK in die Site oder Anwendung erforderlich, oder es ist erforderlich, dass ein Dienstanbieter die Injektion dynamisch durchführt.

Wenn JavaScript Unterstützung erforderlich ist, stellt dies eine zusätzliche Hürde für Bots dar, die versuchen, Browser zu emulieren. Wenn ein SDK involviert ist, z. B. in einer mobilen Anwendung, verifiziert die Token-Erfassung die SDK-Implementierung und verhindert, dass Bots die Anforderungen der Anwendung nachahmen.

Die Token-Akquisition erfordert die Verwendung von, die auf der Client-Seite der Verbindung SDKs implementiert ist. Die folgenden AWS WAF Funktionen bieten ein JavaScript auf Browser basierendes SDK und ein anwendungsbasiertes SDK für mobile Geräte: Bot-Kontrolle, Verhinderung von Kontoübernahmen (ATP) bei der Betrugsbekämpfung und Betrugsprävention bei der Kontoerstellung (ACFP).

Zu den Techniken zur Kundenidentifikation gehören CAPTCHA, Browser-Profiling, Geräte-Fingerprinting und TLS-Fingerprinting.

CAPTCHA

Der vollständig automatisierte öffentliche Turing-Test zur Unterscheidung von Computern und Menschen (CAPTCHA) wird verwendet, um zwischen Robotern und menschlichen Besuchern zu unterscheiden und Web-Scraping, Credential-Stuffing und Spam zu verhindern. Es gibt eine Vielzahl von Implementierungen, aber sie beinhalten oft ein Rätsel, das ein Mensch lösen kann. CAPTCHAsbieten eine zusätzliche Schutzebene gegen häufig vorkommende Bots und können die Zahl der Fehlalarme bei der Bot-Erkennung reduzieren.

AWS WAF ermöglicht Regeln, eine CAPTCHA-Aktion gegen Webanfragen auszuführen, die den Prüfkriterien einer Regel entsprechen. Diese Aktion ist das Ergebnis der Auswertung der vom Dienst gesammelten Kundenidentifikationsinformationen. AWS WAF Regeln können erfordern, dass CAPTCHA-Herausforderungen für bestimmte Ressourcen gelöst werden, die häufig von Bots angegriffen werden, z. B. beim Anmelden, Suchen und Einreichen von Formularen. AWS WAF kann CAPTCHA direkt über interstitielle Mittel oder mithilfe eines SDK bereitstellen, um es auf der Clientseite zu handhaben. Weitere Informationen finden Sie unter CAPTCHA und Challenge in. AWS WAF

Browser-Profilerstellung

Die Erstellung von Browserprofilen ist eine Methode zur Erfassung und Auswertung von Browsermerkmalen im Rahmen der Token-Erfassung, um echte Menschen, die einen interaktiven Browser verwenden, von verteilten Bot-Aktivitäten zu unterscheiden. Sie können Browserprofile passiv anhand von Headern, Header-Reihenfolge und anderen Merkmalen von Anfragen erstellen, die für die Funktionsweise von Browsern typisch sind.

Sie können die Browser-Profilerstellung auch im Code durchführen, indem Sie die Token-Erfassung verwenden. Durch JavaScript die Verwendung von Browserprofilen können Sie schnell feststellen, ob ein Client dies unterstützt. JavaScript Auf diese Weise können Sie einfache Bots erkennen, die dies nicht unterstützen. Die Browser-Profilerstellung überprüft mehr als nur HTTP-Header und deren JavaScript Unterstützung. Die Browser-Profilerstellung erschwert es Bots, einen Webbrowser vollständig zu emulieren. Beide Optionen zur Browser-Profilerstellung verfolgen dasselbe Ziel: Muster in einem Browserprofil zu finden, die auf Inkonsistenzen mit dem Verhalten eines echten Browsers hinweisen.

AWS WAF Die Bot-Kontrolle für gezielte Bots gibt im Rahmen der Token-Auswertung Aufschluss darüber, ob ein Browser Hinweise auf Automatisierung oder inkonsistente Signale aufweist. AWS WAF kennzeichnet die Anfrage, um die in der Regel angegebene Aktion auszuführen. Weitere Informationen finden Sie im AWS Sicherheitsblog unter Erkennen und Blockieren von fortgeschrittenem Bot-Traffic.

Fingerabdruck auf dem Gerät

Das Geräte-Fingerprinting ähnelt der Erstellung von Browserprofilen, ist jedoch nicht auf Browser beschränkt. Code, der auf einem Gerät ausgeführt wird (das kann ein Mobilgerät oder ein Webbrowser sein), sammelt Details des Geräts und meldet sie an einen Backend-Server. Zu den Details können Systemattribute wie Speicher, CPU-Typ, Kerneltyp des Betriebssystems (OS), Betriebssystemversion und Virtualisierung gehören.

Mithilfe von Geräte-Fingerprinting können Sie erkennen, ob ein Bot eine Umgebung emuliert oder ob es direkte Anzeichen dafür gibt, dass Automatisierung verwendet wird. Darüber hinaus kann das Geräte-Fingerprinting auch verwendet werden, um wiederholte Anfragen von demselben Gerät zu erkennen.

Das Erkennen wiederholter Anfragen von demselben Gerät, selbst wenn das Gerät versucht, einige Merkmale der Anfrage zu ändern, ermöglicht es einem Backend-System, Regeln zur Geschwindigkeitsbegrenzung festzulegen. Regeln zur Ratenbegrenzung, die auf Geräte-Fingerprinting basieren, sind in der Regel effektiver als Regeln zur Ratenbegrenzung, die auf IP-Adressen basieren. Auf diese Weise können Sie Bot-Traffic abwehren, der zwischen VPNs Proxys rotiert, aber von einer kleinen Anzahl von Geräten stammt.

In Kombination mit der Anwendungsintegration SDKs kann die AWS WAF Bot-Steuerung für gezielte Bots das Verhalten von Client-Sitzungsanfragen aggregieren. Auf diese Weise können Sie legitime Clientsitzungen erkennen und von böswilligen Clientsitzungen trennen, selbst wenn beide von derselben IP-Adresse stammen. Weitere Informationen zur AWS WAF Bot-Kontrolle für gezielte Bots finden Sie im AWS Sicherheits-Blog unter Erkennen und Blockieren von fortgeschrittenem Bot-Traffic.

TLS-Fingerprinting

TLS-Fingerprinting, auch signaturbasierte Regeln genannt, werden häufig verwendet, wenn Bots von vielen IP-Adressen stammen, aber ähnliche Eigenschaften aufweisen. Bei der Verwendung von HTTPS tauschen Client- und Serverseite Nachrichten aus, um sich gegenseitig zu bestätigen und zu verifizieren. Sie richten kryptografische Algorithmen und Sitzungsschlüssel ein. Dies wird als

TLS-Handshake bezeichnet. Die Art und Weise, wie ein TLS-Handshake implementiert wird, ist eine Signatur, die oft nützlich ist, um große Angriffe zu erkennen, die sich über viele IP-Adressen verteilen.

Mithilfe von TLS-Fingerprinting können Webserver die Identität eines Webclients mit hoher Genauigkeit ermitteln. Es erfordert nur die Parameter in der ersten Paketverbindung, bevor ein Anwendungsdatenaustausch stattfindet. In diesem Fall bezieht sich Webclient auf die Anwendung, die eine Anfrage initiiert. Dabei kann es sich um einen Browser, ein CLI-Tool, ein Skript (Bot), eine native Anwendung oder einen anderen Client handeln.

Ein Ansatz für das SSL- und TLS-Fingerprinting ist JA3 der Fingerabdruck. JA3gibt anhand von Feldern in der Client Hello-Nachricht aus dem SSL- oder TLS-Handshake einen Fingerabdruck auf eine Client-Verbindung ab. Es hilft Ihnen, Profile für bestimmte SSL- und TLS-Clients anhand verschiedener Quell-IP-Adressen, Ports und X.509-Zertifikate zu erstellen.

Amazon CloudFront unterstützt das Hinzufügen von JA3 Headern zu Anfragen. Ein `CloudFront-Viewer-JA3-Fingerprint` Header enthält einen 32-stelligen Hash-Fingerabdruck des TLS-Client-Hello-Pakets einer eingehenden Viewer-Anfrage. Der Fingerabdruck enthält Informationen darüber, wie der Client kommuniziert. Diese Informationen können verwendet werden, um Profile von Clients zu erstellen, die dasselbe Muster verwenden. Sie können den `CloudFront-Viewer-JA3-Fingerprint` Header zu einer ursprünglichen Anforderungsrichtlinie hinzufügen und die Richtlinie einer CloudFront Distribution zuordnen. Sie können den Header-Wert dann in Originalanwendungen oder in Lambda @Edge und CloudFront Functions überprüfen. Sie können den Header-Wert mit einer Liste bekannter Malware-Fingerabdrücke vergleichen, um bösartige Clients zu blockieren. Sie können den Header-Wert auch mit einer Liste erwarteter Fingerabdrücke vergleichen, um nur Anfragen von bekannten Clients zuzulassen.

Erweiterte Analysefunktionen für die Verwaltung von Bots

Einige Bots verwenden fortschrittliche Täuschungstools, um sich aktiv der Entdeckung zu entziehen. Diese Bots ahmen menschliches Verhalten nach, um eine bestimmte Aktivität wie Scalping auszuführen. Diese Bots haben einen Zweck, der normalerweise mit einer großen finanziellen Belohnung verbunden ist.

Diese fortschrittlichen, persistenten Bots verwenden eine Mischung von Technologien, um der Entdeckung zu entgehen oder sich in den regulären Traffic einzumischen. Dies wiederum erfordert auch eine Mischung verschiedener Erkennungstechnologien, um den bösartigen Datenverkehr genau zu identifizieren und einzudämmen.

Gezielte Anwendungsfälle

Anwendungsfalldaten können Möglichkeiten zur Bot-Erkennung bieten. Bei Betrugserkennungen handelt es sich um spezielle Anwendungsfälle, bei denen besondere Maßnahmen erforderlich sind. Um beispielsweise Kontoübernahmen zu verhindern, können Sie eine Liste kompromittierter Kontonutzernamen und Passwörter mit Anfragen zur Anmeldung oder Kontoerstellung vergleichen. Dies hilft Website-Besitzern, Anmeldeversuche zu erkennen, bei denen kompromittierte Anmeldeinformationen verwendet werden. Die Verwendung kompromittierter Anmeldeinformationen kann darauf hindeuten, dass Bots versuchen, ein Konto zu übernehmen, oder es könnten Benutzer sein, die nicht wissen, dass ihre Anmeldeinformationen kompromittiert wurden. In diesem Anwendungsfall können Webseitenbesitzer zusätzliche Schritte unternehmen, um den Benutzer zu verifizieren und ihm dann zu helfen, sein Passwort zu ändern. AWS WAF stellt die verwaltete Regel zur Verhinderung von Kontoübernahmen (Fraud Control Account Takeover Prevention, ATP) für diesen Anwendungsfall bereit.

Bot-Erkennung auf Anwendungsebene oder aggregierte Bot-Erkennung

In einigen Anwendungsfällen müssen Daten über Anfragen aus dem Content Delivery Network (CDN) und dem Backend der Anwendung oder des Dienstes kombiniert werden. AWS WAF Manchmal müssen Sie sogar Informationen von Drittanbietern integrieren, um fundierte Entscheidungen über Bots treffen zu können.

Funktionen in Amazon CloudFront und AWS WAF können Signale an die Backend-Infrastruktur senden oder Regeln anschließend über Header und Labels aggregieren. CloudFront macht, wie bereits erwähnt, JA3 Fingerabdruck-Header verfügbar. Dies ist ein Beispiel für CloudFront die Bereitstellung solcher Daten über einen Header. AWS WAF kann Labels senden, wenn es einer Regel entspricht. Nachfolgende Regeln können diese Labels verwenden, um bessere Entscheidungen über Bots zu treffen. Wenn mehrere Regeln kombiniert werden, können Sie sehr detaillierte Kontrollen implementieren. Ein häufiger Anwendungsfall besteht darin, Teile einer verwalteten Regel anhand eines Labels abzugleichen und diese dann mit anderen Anforderungsdaten zu kombinieren. Weitere Informationen finden Sie in der AWS WAF Dokumentation unter Beispiele für den Label-Abgleich.

Analyse des maschinellen Lernens

Machine Learning (ML) ist eine leistungsstarke Technik für den Umgang mit Bots. ML kann sich an sich ändernde Details anpassen und bietet in Kombination mit anderen Tools die robusteste und vollständigste Methode zur Abwehr von Bots mit minimalen Fehlalarmen. Die beiden gängigsten ML-

Techniken sind die Verhaltensanalyse und die Erkennung von Anomalien. Bei der Verhaltensanalyse überwacht ein System (im Client, Server oder in beiden), wie ein Benutzer mit der Anwendung oder Website interagiert. Es überwacht Mausbewegungsmuster oder die Häufigkeit von Klick- und Berührungsinteraktionen. Das Verhalten wird dann mit einem ML-Modell analysiert, um Bots zu erkennen. Die Erkennung von Anomalien ist ähnlich. Der Schwerpunkt liegt auf der Erkennung von Verhaltensweisen oder Mustern, die sich erheblich von einer für die Anwendung oder Website definierten Ausgangsbasis unterscheiden.

AWS WAF Gezielte Kontrollen für Bots bieten prädiktive ML-Technologie. Diese Technologie trägt zur Abwehr verteilter, proxybasierter Angriffe bei, die von Bots ausgeführt werden, die darauf ausgelegt sind, der Entdeckung zu entgehen. Die Regelgruppe Managed AWS WAF Bot Control verwendet automatisierte ML-Analysen der Statistiken zum Website-Traffic, um ungewöhnliches Verhalten zu erkennen, das auf verteilte, koordinierte Bot-Aktivitäten hindeutet.

Implementierung und Implementierung Ihrer Bot-Kontrollstrategie

Bei der Planung einer Implementierungsstrategie zur Bot-Steuerung sind mehrere Faktoren zu berücksichtigen. Neben den einzigartigen Eigenschaften von Webanwendungen wirken sich auch die Größe der Umgebung, der Entwicklungsprozess und die Organisationsstruktur auf die Bereitstellungsstrategie aus. Je nach Umgebung und Anwendungsmerkmalen kann eine zentralisierte oder dezentrale Bereitstellungsstrategie verwendet werden:

- Zentralisierte Bereitstellungsstrategie — Ein zentralisierter Ansatz ermöglicht ein höheres Maß an Kontrolle, wenn Sie die Bot-Kontrolle strikt durchsetzen möchten. Dieser Ansatz ist gut geeignet, wenn Anwendungsteams es vorziehen, die Verwaltung auszulagern. Ein zentralisierter Ansatz ist am effektivsten, wenn Webanwendungen ähnliche Merkmale aufweisen. In diesem Fall profitieren die Anwendungen von einem gemeinsamen Satz von Regeln zur Bot-Kontrolle und Maßnahmen zur Bot-Abwehr.
- Dezentrale Bereitstellungsstrategie — Ein dezentraler Ansatz bietet Anwendungsteams die Möglichkeit, Konfigurationen zur Bot-Steuerung unabhängig voneinander zu definieren und zu implementieren. Dieser Ansatz ist in kleineren Umgebungen üblich oder wenn Anwendungsteams die Kontrolle über ihre Bot-Kontrollrichtlinien behalten müssen. Aufgrund der Beschaffenheit vieler Webanwendungen ist es oft erforderlich, unabhängige Richtlinien zur Bot-Steuerung beizubehalten, die auf einzigartige Anwendungsmerkmale zugeschnitten sind, was zu einem dezentralen Ansatz führt.
- Kombinierte Strategie — Eine Kombination dieser beiden Ansätze ist für eine Mischung von Webanwendungen geeignet. Dies kann beispielsweise eine Reihe von Grundregeln beinhalten, die für alle Websites gelten ACLs, während die Verwaltung spezifischerer Richtlinien zur Bot-Kontrolle an Anwendungsteams delegiert wird.

Sie können AWS Firewall Managerdamit die Bereitstellung von AWS WAF Webanwendungen zentralisieren und automatisieren ACLs , die Richtlinien zur Bot-Kontrolle definieren. Überlegen Sie sich bei der Verwendung von Firewall Manager, ob es angemessen ist, die Richtlinien zur Bot-Kontrolle zu zentralisieren, und ob diese auch an Anwendungsteams delegiert werden sollten. Mit Firewall Manager können Sie Tagging verwenden, um es Anwendungsteams zu ermöglichen, sich für AWS WAF Richtlinien zu entscheiden. Dies bietet intelligente Funktionen AWS WAF zur Bedrohungsabwehr. Sie können auch die zentrale AWS WAF Protokollierung für Anwendungs- und Sicherheitsvorgänge aktivieren.

Unabhängig von der verwendeten Implementierungsstrategie wird empfohlen, den Onboarding-Prozess mithilfe von Infrastructure-as-Code (IaC) -basierten Frameworks wie AWS CloudFormationoder dem zu definieren und zu verwalten. AWS Cloud Development Kit (AWS CDK) Auf diese Weise können Sie die Quellcodeverwaltung so konfigurieren, dass Konfigurationsobjekte gespeichert und versioniert werden. Weitere Informationen finden Sie in den AWS WAF Konfigurationsbeispielen für AWS CDK(GitHub) und CloudFormation(AWS Dokumentation).

Strategie für die Implementierung

Nachdem Sie eine Bereitstellungsstrategie ausgewählt haben, kann die Implementierung beginnen. Die Bereitstellungsstrategie definiert, wie Regeln für verschiedene Anwendungen eingeführt werden. In der Implementierungsstrategie liegt der Schwerpunkt auf dem iterativen Prozess, bei dem Kontrollen hinzugefügt, getestet, kontinuierlich überwacht und anschließend deren Auswirkungen bewertet werden.

Verkehrsmuster verstehen

Um Verkehrsmuster wirklich zu verstehen, ist es wichtig, sich mit der Geschäftsfunktion der Anwendung und den erwarteten Attributen wie Nutzungsmustern, wichtigen Ressourcen und Benutzerpersönlichkeiten vertraut zu machen. Integrieren Sie den Produktionsdatenverkehr und den Datenverkehr, der während der Tests mit der Anwendung generiert wurde, um eine Ausgangsbasis für die Bewertung zu erstellen. Stellen Sie sicher, dass der Zeitrahmen Verkehrsdaten enthält, die mehrere Nutzungsspitzen ausreichend abbilden.

Überprüfen Sie mit Ihrem bevorzugten Tool die Verkehrsprotokolle und Messwerte für den jeweiligen Nutzungszeitraum. Analysieren AWS WAF Sie die Protokolldaten auf ungewöhnliche Anfragen, indem Sie nach Protokollfeldern wie `headers` (zum Beispiel `User-Agent` und`Referer`)`country`, und filtern. `clientIp` Notieren Sie sich die einheitlichen Ressourcenkennungen (URIs) und deren Zugriffshäufigkeit. Kategorisieren Sie den Traffic, z. B. die Identifizierung guter Bots. Erlauben Sie beispielsweise nützlichen Bots wie Suchmaschinen-Crawlern und Monitoren den Zugriff.

In der AWS WAF Konsole, im Dashboard zur Bot-Kontrolle, ist ein Beispiel für Bot-Aktivitäten für jede aktive Web-ACL verfügbar. Dies bietet zwar einen ersten Überblick über das Volumen der häufigsten Bot-Anfragen, aber führen Sie weitere Konfigurationen und Analysen durch, um die Bot-Aktivitäten besser zu verstehen.

Für eine effektive Implementierung müssen Sie ein gutes Verständnis des Bot-Traffics und seiner Auswirkungen haben und wissen, welche Bot-Anfragen nützlich und welche bösartig sind. Dies hilft

bei der nächsten Phase, der Auswahl von Steuerelementen, und hilft Ihnen, den Bot-Traffic parallel auszuwerten.

Steuerelemente auswählen und hinzufügen

Anhand der ersten Verkehrsanalyse kann bestimmt werden, welche Bot-Steuerelemente verwendet werden sollen und welche Aktionen für welche ausgewählt werden müssen. Sie können sich auch dafür entscheiden, Aktivitäten zu protokollieren und zu überwachen, um mögliche future Maßnahmen zu ergreifen. Die erste Verkehrsanalyse hilft Ihnen dabei, die beste Steuerung für die Verwaltung des Datenverkehrs auszuwählen. Weitere Informationen zu den verfügbaren Steuerungen finden Sie Techniken zur Bot-Kontrolle in diesem Handbuch.

Erwägen Sie, in diesem Schritt zusätzliche SDK-Implementierungen einzubeziehen. Auf diese Weise können Sie SDK-Implementierungen in allen erforderlichen Anwendungen testen und abschließen. AWS WAF Regeln zur Bot-Kontrolle und Betrugsbekämpfung bieten einen umfassenden Vorteil bei der Token-Evaluierung, wenn Sie ein JavaScript SDK oder ein SDK für Mobilgeräte implementieren. Weitere Informationen finden Sie in der AWS WAF Dokumentation unter Warum Sie die Anwendungsintegration SDKs mit Bot Control verwenden sollten.

Wir empfehlen, die Token-Akquisition für verschiedene Anwendungstypen wie folgt zu implementieren:

- Einseitige Anwendung (SPA) — JavaScript SDK (keine Weiterleitung)
- Mobiler Browser — JavaScript SDK- oder Regelaktionen (CAPTCHA oder Challenge)
- Webansichten — JavaScript SDK- oder Regelaktionen (CAPTCHA oder Challenge)
- Native Anwendungen — SDK für Mobilgeräte
- iFrames — SDK JavaScript

Weitere Informationen zur Implementierung von finden Sie in der SDKs AWS WAF Dokumentation unter Integration von AWS WAF Client-Anwendungen.

Testen und Bereitstellen in der Produktion

Die Steuerelemente sollten zunächst in einer Produktionsumgebung bereitgestellt werden, in der Sie Tests durchführen können, um sicherzustellen, dass die erwartete Funktionalität der Webanwendung erhalten bleibt. Führen Sie vor der Bereitstellung in der Produktion immer eine gründliche Validierung in einer Testumgebung durch.

Nach dem Testen und Validieren in einer Umgebung außerhalb der Produktionsumgebung kann mit der Produktionsversion fortgefahren werden. Wählen Sie ein Datum und eine Uhrzeit mit dem geringsten erwarteten Benutzerverkehr aus. Vor der Implementierung sollten die Anwendungs- und Sicherheitsteams die Betriebsbereitschaft überprüfen, besprechen, wie Änderungen rückgängig gemacht werden können, und die Dashboards überprüfen, um sicherzustellen, dass alle erforderlichen Metriken und Alarme konfiguriert sind.

Mit Amazon CloudFront Continuous Deployment können Sie eine geringe Menge an Traffic an eine Staging-Distribution senden, für die eine AWS WAF Web-ACL speziell für die Auswertung der Bot-Kontrolle konfiguriert ist. AWS WAF bietet die Versionsverwaltung aller neuen oder aktualisierten verwalteten Regeln, sodass Sie Änderungen testen und genehmigen können, bevor sie mit der Auswertung des Produktionsverkehrs beginnen.

Evaluierung und Optimierung von Steuerungen

Implementierte Kontrollen können weitere Einblicke und Einblicke in die Verkehrsaktivitäten und -muster bieten. Überwachen und analysieren Sie häufig den Anwendungsdatenverkehr, um Sicherheitskontrollen hinzuzufügen oder anzupassen. Normalerweise gibt es eine Phase der Optimierung, um mögliche falsch negative und falsch positive Ergebnisse zu vermeiden. Falsch negative Angriffe sind Angriffe, die nicht von Ihren Kontrollen erfasst wurden und bei denen Sie Ihre Regeln verschärfen müssen. Falsch positive Ergebnisse stehen für legitime Anfragen, die fälschlicherweise als Angriffe identifiziert und infolgedessen blockiert wurden.

Die Analyse und das Tuning können manuell oder mit Hilfe von Tools erfolgen. Ein SIEM-System (Security Information and Event Management) ist ein gängiges Tool, das zur Bereitstellung von Kennzahlen und intelligenter Überwachung beiträgt. Es gibt viele davon mit unterschiedlichem Grad an Raffinesse, aber sie bieten alle einen guten Ausgangspunkt, um Einblicke in den Verkehr zu erhalten.

Durch die Definition wichtiger Leistungsindikatoren (KPIs) für Websites und Anwendungen können Sie schneller erkennen, wann etwas nicht wie erwartet funktioniert. Beispielsweise können Sie Kreditkartenrückbuchungen, Verkäufe pro Konto oder Konversionsraten als Indikatoren für Geschäftsanomalien verwenden, die durch Bots generiert werden können. Es ist sogar noch wichtiger, zu definieren und zu verstehen, welche Kennzahlen für die Überwachung wertvoll KPIs sind, als nur die eigentliche Überwachung.

Zu verstehen, wie man mit einer Bot-Kontrolllösung die richtigen Metriken und Logs erhält, ist genauso wichtig wie die Identifizierung der zu überwachenden Metriken. Im nächsten Abschnitt

werden die zu berücksichtigenden Überwachungs- und Sichtbarkeitsoptionen beschrieben.
Richtlinien für die Überwachung Ihrer Bot-Kontrollstrategie

Richtlinien für die Überwachung Ihrer Bot-Kontrollstrategie

Für den Bot-Traffic und den Traffic von Webanwendungen sind Überwachung und Sichtbarkeit von großer Bedeutung. Es hilft Ihnen, Aktivitäten und Sicherheitsoperationen zu priorisieren. Wenn eine detaillierte Protokollierung oder die Verwendung eines SIEM-Systems nicht möglich sind, ist die Überwachung grundlegender Kennzahlen, die von Ihrer ausgewählten Lösung oder Ihrem Anbieter bereitgestellt werden, ein guter Ausgangspunkt.

Diese Transparenz ist nützlich, um Bedrohungsinformationen zu sammeln, Regeln zu verschärfen, Fehlalarme zu beheben und auf einen Vorfall zu reagieren. Es stehen mehrere Überwachungsoptionen mit zur Verfügung AWS WAF. Für die Überwachung auf hoher Ebene AWS WAF bietet es Informationen zur Verkehrsübersicht im AWS-Managementkonsole. Diese Option ist für den gesamten Datenverkehr sowie eine detaillierte Ansicht für den Bot-Verkehr verfügbar, sofern die Regelgruppe Bot Control in Ihrer Web-ACL aktiviert ist.

AWS WAF bietet verschiedene Optionen für die detaillierte Protokollierung des Web-ACL-Datenverkehrs. Sie können Anfragen auch Labels hinzufügen, die Sie verwenden können, um die Protokollanalyse zu vereinfachen und Regeln für die Bot-Auswertung zu konfigurieren. Durch die Integration von Amazon CloudWatch Logs Insights können Sie die AWS WAF Protokolle abfragen und die Ergebnisse visualisieren.

Wenn Sie die detaillierte Protokollierung aktivieren, AWS WAF bietet dies zusätzliche Einblicke, die über das vorkonfigurierte Dashboard zur Bot-Kontrolle hinausgehen. Die Verwendung von AWS WAF Protokollen zur Visualisierung des Datenverkehrs sowie Ad-hoc-Untersuchungen können zu einem umfassenden Verständnis der Verkehrsmuster und der Optionen zur Risikominderung für eine Webanwendung führen.

Sie können AWS WAF Protokolldaten mit Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3) oder Amazon Data Firehose integrieren. Weitere Informationen finden Sie unter AWS WAF Protokollierung aktivieren und Protokolle an CloudWatch Amazon S3 oder Amazon Data Firehose senden. Sie können Protokolle auch zur Analyse an verschiedene Ziele senden, z. B. an Amazon OpenSearch Service oder eine AWS MarketplaceLösung. Weitere Informationen finden Sie unter Zieleinstellungen in der Firehose-Dokumentation. Wenn mehrere Protokollquellen verwendet werden, wird eine zentralisierte Protokollierungslösung empfohlen, um die Quellen zu korrelieren.

Als Nächstes enthält dieser Leitfaden Empfehlungen, wie Sie mit der Überwachung des Bot-Traffics beginnen und mithilfe von Amazon Transparenz gewinnen können CloudWatch.

Die wichtigsten Regeln verfolgen

Durch die Nachverfolgung der am häufigsten aufgerufenen Regeln können Trends und potenziell ungewöhnliche Aktivitäten aufgedeckt werden. Erhöhte Raten für eine bestimmte Regel könnten auf eine potenzielle falsch positive oder gezielte Aktivität hinweisen, die Sie untersuchen sollten. Die gängigste Regel für Tracking wären IP-basierte Steuerungen Geoblocking-Regeln (ein Anstieg kann hier Traffic aus ungewöhnlichen Ländern anzeigen, die möglicherweise nicht automatisch blockiert werden) und. Ratenbasierte Regeln Diese Regeln würden immer von Natur aus variieren, aber eine Anomalie im Verkehrsmuster kann auf Bot-Aktivitäten hinweisen. Berücksichtigen Sie dies, wenn Sie die Schwellenwerte manuell festlegen.

Nachverfolgung der wichtigsten Labels und Namespaces

Mithilfe von CloudWatch Metriken können Sie die am häufigsten verwendeten Labels nachverfolgen, welche AWS WAF Regeln häufig aufgerufen werden. Auf diese Weise können Sie Anomalien wie eine Zunahme der Scraper-Aktivität, Traffic aus verdächtigen Quellen oder versuchten Missbrauch der Anmeldeseite oder der API der Anwendung erkennen.

Im Folgenden finden Sie Beispiele für Labels, die von Interesse sein könnten:

- `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`

Im Folgenden finden Sie Beispiele für Label-Namespaces, die von Interesse sein könnten:

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

Mathematische Ausdrücke erstellen

In Amazon CloudWatch können Sie mathematische Ausdrücke für eine oder alle Regeln erstellen. Wenn Sie Warnmeldungen für mathematische Ausdrücke einrichten, werden Sie über Abweichungen bei den Raten, nicht bei den Mengen, bei bestimmten Kennzahlen informiert. Dies ist ein wichtiges Instrument zur Verringerung der Alarmmüdigkeit.

Erstellen Sie eine benutzerdefinierte Metrik, die aus einem mathematischen Ausdruck besteht. Schauen Sie sich die relativen Raten für Regeln an, gemessen an der Gesamtzahl der Anfragen an eine Anwendung. Der folgende mathematische Ausdruck ist gebräuchlich:

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

Dieser mathematische Ausdruck gibt einen Prozentsatz an, sodass Sie eine bestimmte Regel verfolgen und ihren Trend im Laufe der Zeit visualisieren können.

Verwenden der Anomalieerkennung

Wenn Sie die CloudWatchAnomalieerkennung für eine beliebige CloudWatch Metrik verwenden, können Sie Warnmeldungen bei ungewöhnlich niedrigen oder hohen Trends ausgeben, ohne den tatsächlichen Schwellenwert manuell einrichten zu müssen. Diese Algorithmen analysieren kontinuierlich Metriken von Systemen und Anwendungen, ermitteln normale Ausgangswerte und decken Anomalien mit minimalem Benutzereingriff auf. CloudWatch wendet in seiner Funktion zur Erkennung von Anomalien statistische Algorithmen und ML-Algorithmen an.

Verwenden von CloudWatch Amazon-Metriken

AWS WAF verarbeitet den Datenverkehr und fügt Anfragen, die den in der Web-ACL definierten Regeln entsprechen, Labels hinzu. Jedes Label erstellt eine Metrik in CloudWatch. Gleichzeitig erstellt jede Web-ACL-Regel auch Metriken für jede ihrer möglichen Aktionen. Verwenden Sie diese Kennzeichnungs- und Aktionsmetriken, um sich einen umfassenden Überblick über den Bot-Traffic zu verschaffen. Dies ist ein kostengünstiger Ansatz zur Visualisierung von Trends. Weitere Informationen finden Sie in der Dokumentation unter Verfügbare Metriken anzeigen und Metriken grafisch darstellen. CloudWatch

CloudWatch bietet die Möglichkeit, Daten an einen Protokollsammler oder Aggregator zu senden, unabhängig davon, ob es sich um eine Lösung AWS-Service oder eine Drittanbieterlösung handelt. Die Erfassung von Daten ermöglicht eine CloudWatch konsolidiertere Sicherheitsbeobachtbarkeit,

bei der Sie Daten aus mehreren Quellen korrelieren können. Dies kann Ihnen helfen, Ihre Warnmeldungen und Sicherheitsautomatisierungen zu untersuchen, einzusehen oder einzurichten.

Aufbau eines Dashboards

Nachdem Sie die wichtigen Kennzahlen identifiziert haben, die Sie verfolgen möchten, erstellen Sie ein Dashboard, das die relevantesten Kennzahlen enthält. Ihre Anzeige side-by-side unter einer einzigen Glasscheibe kann für zusätzliche Transparenz und Kontrolle sorgen.

Es ist immer vorzuziehen, Warnmeldungen und Automatisierungsregeln für anomale Metrikwerte zu konfigurieren. Verlassen Sie sich nicht darauf, dass Menschen Anomalien anhand eines Dashboards erkennen. Dashboards können jedoch für Untersuchungszwecke nützlich sein, nachdem eine Warnung eingegangen ist.

Optimierung der Kosten für Ihre Bot-Kontrollstrategie

Der Web-Traffic ist von Natur aus dynamisch. Das bedeutet, dass die Technologien und Dienste, die zur Abwehr von Bedrohungen eingesetzt werden, variieren und im Laufe der Zeit angepasst werden können. Dies ist entscheidend, wenn man eine Strategie zur Bot-Kontrolle und die darin enthaltenen Kontrollen in Betracht zieht. Die Optimierung im Laufe der Zeit ist das wichtigste Prinzip, das es zu beachten gilt, und es stammt aus der Säule der Kostenoptimierung des AWS Well-Architected Framework.

AWS WAF Das Web ACLs kann dynamisch sein, insbesondere wenn neue Funktionen veröffentlicht werden oder wenn Sie versuchen, eine neue Bedrohung abzuwehren. Um Ihre Kosten im Auge zu behalten, müssen Sie die Kostendimensionen des AWS WAF Services verstehen und wissen, wie sich diese auf Ihre endgültigen Ausgaben auswirken. Der Hauptkostenfaktor ist die Anzahl der Anfragen, die vom Service bewertet werden. Zusätzliche Gebühren fallen an, wenn Sie die verwalteten Regelgruppen Bot Control und Account Takeover Prevention (ATP) oder erweiterte Aktionen wie CAPTCHA oder Challenge verwenden.

Da spezielle Bot-Kontrollen mit hohen Kosten verbunden sind, besteht das primäre Ziel der Kostenoptimierung darin, die Anzahl der Anfragen zu reduzieren, die durch diese erweiterten Kontrollen geprüft werden. Zu den anwendbaren Techniken gehören die Trennung hochwertiger Inhalte, die Anwendung kostengünstigerer Maßnahmen, die Eingrenzung des Bewertungsbereichs und die Kombination von Bot-Schutz mit anderen Arten von Kontrollen. Techniken zur Kostenüberwachung sorgen für zusätzliche Transparenz in Ihrem gesamten Unternehmen.

Trennung von dynamischen und statischen Inhalten

Eine Methode zur Kostensenkung besteht darin, den statischen Inhalt von der dynamischen Anwendung zu isolieren. Die meisten Anfragen an typische Webanwendungen sind Anfragen an statische Objekte. Eine gängige Methode, um die Belastung von Anwendungsservern zu reduzieren, besteht darin, statische Inhalte auf eine eigene URL zu verschieben, z. `static.example.com` B. Dies wird häufig erreicht, indem eine einzigartige Verteilung für die Inhaltsbereitstellung erstellt wird, wobei die Caching-Konfiguration für statische Inhalte optimiert ist. Diese Technik kann auch dazu beitragen, die Kosten für die Bot-Kontrolle zu senken, wenn statische Inhalte auf der Website oder Anwendung nicht häufig als Ziel verwendet werden. Die Trennung des statischen Inhalts von der dynamischen Anwendung kann eine genauere Anwendung erweiterter Bot-Steuerelemente ermöglichen.

Wenden Sie zuerst kostengünstigere Regeln an

Eine andere Methode besteht darin, kostengünstigere Basisregeln anzuwenden, die unerwünschter Datenverkehr herausfiltern, bevor erweiterte Steuerungen verwendet werden, die teurer sind. In der Praxis bedeutet dies in der Regel, die Abwehr der Bot-Kontrolle als letzte Verteidigungsebene einzusetzen und vorangehende Kontrollen zu verwenden, um unerwünschten Datenverkehr herauszufiltern. Dieser Pyramidenansatz wurde bereits Techniken zur Bot-Kontrolle in diesem Leitfaden erörtert. Das Hauptziel besteht darin, diese kostengünstigeren Optionen zu nutzen, um unerwünschten Datenverkehr zu unterbinden und so die Anzahl der Anfragen zu reduzieren, die mit fortschrittlichen, kostenintensiveren Abhilfemaßnahmen bearbeitet werden.

Abgrenzung des Bewertungsbereichs

AWS WAFScope-down-Aussagen bieten eine wirksame Methode, um die Anzahl der Anfragen zu reduzieren, die nach fortgeschrittenen Regeln geprüft werden. Wenn die Trennung statischer Inhalte in eigene URLs nicht implementiert werden kann, sind Scopedown-Anweisungen eine weitere Methode, um Anfragen herauszufiltern, für die keine fortgeschrittenen Abhilfemaßnahmen erforderlich sind. Dies kann durch die Definition eines bestimmten Anwendungspfads, einer HTTP-Methode (wie POST) oder einer ähnlichen Kombination erreicht werden.

Kombination von Bot-Schutz mit anderen Kontrollen

Beim Schutz von Anwendungen vor mehreren Bedrohungen sowie vor unerwünschtem Bot-Traffic sollten zusätzliche Überlegungen zur Kostenkontrolle berücksichtigt werden. Beispielsweise erfordert der Schutz vor Distributed-Denial-of-Service (DDoS) -Angriffen und vor Kontoübernahme zusätzliche Konfigurationen, die sich auf die Kosten auswirken können. Shield Advanced wird empfohlen, um Anwendungen vor DDo S-Angriffen zu schützen. Insbesondere die Schutzmaßnahmen auf Anwendungsebene können die Flut von Anfragen automatisch beheben und so die Anzahl der Anfragen reduzieren, die von der Regelgruppe AWS WAF Bot Control bearbeitet werden können, wenn die Regel in der Bewertungsreihenfolge an erster Stelle steht. Shield Advanced bietet einen zusätzlichen Vorteil: Für verwaltete Standardregeln und benutzerdefinierte AWS WAF Regeln fallen für Ressourcen, die durch Shield Advanced geschützt sind, keine zusätzlichen Kosten an. Beachten Sie, dass Regelgruppen zur intelligenten Bedrohungsabwehr, einschließlich Bot Control, zusätzliche Kosten verursachen, selbst für Ressourcen, die durch Shield Advanced geschützt sind.

Anwendungen, die den Schutz vor Kontoübernahmen erfordern, können die ATP-Regelgruppe (AWS WAF Fraud Control Account Takeover Prevention) verwenden. Die Inspektionskosten pro Anfrage

für die ATP-Regelgruppe sind höher als für die Regelgruppe Bot Control. Aufgrund dieser höheren Kosten ist es wichtig, die ATP-Regelgruppe so präzise wie möglich anzuwenden. Die Verwendung der Bot-Control-Regelgruppe in Verbindung mit ATP kann dazu beitragen, dieses Ziel zu erreichen. Die Regelgruppe Bot Control sollte in der Web-ACL vor ATP platziert werden, um Bot-Anfragen herauszufiltern und die Anzahl der von ATP überprüften Anfragen zu reduzieren.

Für eine kontinuierliche Optimierung besteht die wichtigste Aktivität in der Überwachung von CloudWatchMetriken, die mit der Bot-Control-Regelgruppe verknüpft sind. Das Ziel besteht im Laufe der Zeit darin, die Anzahl der Anfragen, die von der Bot-Control-Regelgruppe bewertet werden, auf diejenigen zu reduzieren, die auf die Ressourcen abzielen, die Sie zum Schutz vor unerwünschten Bot-Aktivitäten benötigen. Die Erstellung von CloudWatch Dashboards bietet Einblick in die wichtigsten Kennzahlen für Anwendungen, einschließlich AWS WAF Kosten und Nutzung.

Überwachung der Kosten

AWS Cost Explorer ist ein Tool, mit dem Sie Ihre Kosten und Nutzung ansehen und analysieren können. Der Cost Explorer erleichtert die Analyse der AWS Kosten, einschließlich der angefallenen AWS WAF Kosten. Das Tool bietet Kosteninformationen für die letzten 12 Monate und prognostiziert future Ausgaben für die nächsten 12 Monate.

AWS Die Erkennung von Kostenanomalien ist ein weiteres Instrument zur Kostenkontrolle, das für die AWS WAF Kostenüberwachung nützlich sein kann. Es verwendet fortschrittliche ML-Technologien, um ungewöhnliche Ausgaben und deren Ursachen zu identifizieren. Auf diese Weise können Sie schnell Maßnahmen ergreifen oder Benachrichtigungen erhalten, wenn es zu einem unerwarteten Kostenanstieg kommt. Um eine Warnung zu erhalten, wenn ein bestimmter Kostenschwellenwert erreicht wird, AWS Budgetskann diese Nachverfolgungs- und Überwachungsfunktion bereitgestellt werden.

Ressourcen

AWS Dokumentation

- AWS WAF Leitfaden für Entwickler
- AWS Bewährte Methoden für DDoS-Resilienz (AWS Whitepapers)
- Richtlinien für die Implementierung (Whitepapers) AWS WAFAWS

Andere Ressourcen AWS

- Analysieren von AWS WAF Protokollen in Amazon CloudWatch Logs (AWS Blogbeitrag)
- Stellen Sie AWS WAF mit minimalem Aufwand ein Dashboard bereit (AWS Blogbeitrag)
- Sicherheitsautomatisierungen für AWS WAF (AWS Lösungsbibliothek)
- Die drei wichtigsten AWS WAF ratenbasierten Regeln (AWS Blogbeitrag)
- AWS WAF Logs mit einem CloudWatch Amazon-Dashboard visualisieren (AWS Blogbeitrag)

Mitwirkende

Inhaltserstellung

- Diana Alvarado, leitende Lösungsarchitektin, AWS
- Cameron Worrell, Unternehmensarchitekt, AWS
- Geary Scherer, Lösungsarchitekt, AWS
- Tzoori Tamam, Hauptarchitekt für Lösungen, AWS

Überprüfend

- Jess Izen, leitender Softwareentwicklungsingenieur, AWS
- Kaustubh Phatak, leitender Produktmanager, AWS
- Vikramaditya Bhatnagar, leitender Sicherheitsberater, AWS

Technisches Schreiben

- Lilly AbouHarb, leitende technische Redakteurin, AWS

Dokumentverlauf

In der folgenden Tabelle werden wichtige Änderungen in diesem Leitfaden beschrieben. Um Benachrichtigungen über zukünftige Aktualisierungen zu erhalten, können Sie einen RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Erste Veröffentlichung	—	21. Februar 2024

AWS Glossar zu präskriptiven Leitlinien

Die folgenden Begriffe werden häufig in Strategien, Leitfäden und Mustern verwendet, die von AWS Prescriptive Guidance bereitgestellt werden. Um Einträge vorzuschlagen, verwenden Sie bitte den Link Feedback geben am Ende des Glossars.

Zahlen

7 Rs

Sieben gängige Migrationsstrategien für die Verlagerung von Anwendungen in die Cloud. Diese Strategien bauen auf den 5 Rs auf, die Gartner 2011 identifiziert hat, und bestehen aus folgenden Elementen:

- Refactor/re-architect — Verschieben Sie eine Anwendung und ändern Sie ihre Architektur, indem Sie alle Vorteile der Cloud-nativen Funktionen nutzen, um Agilität, Leistung und Skalierbarkeit zu verbessern. Dies beinhaltet in der Regel die Portierung des Betriebssystems und der Datenbank. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank auf die Amazon Aurora PostgreSQL-Compatible Edition.
- Plattformwechsel (Lift and Reshape) – Verschieben Sie eine Anwendung in die Cloud und führen Sie ein gewisses Maß an Optimierung ein, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Amazon Relational Database Service (Amazon RDS) für Oracle in der. AWS Cloud
- Neukauf (Drop and Shop) – Wechseln Sie zu einem anderen Produkt, indem Sie typischerweise von einer herkömmlichen Lizenz zu einem SaaS-Modell wechseln. Beispiel: Migrieren Sie Ihr Kundenbeziehungsmanagement (CRM) -System zu. Salesforce.com
- Hostwechsel (Lift and Shift) – Verschieben Sie eine Anwendung in die Cloud, ohne Änderungen vorzunehmen, um die Cloud-Funktionen zu nutzen. Beispiel: Migrieren Sie Ihre lokale Oracle-Datenbank zu Oracle auf einer EC2-Instanz in der. AWS Cloud
- Verschieben (Lift and Shift auf Hypervisor-Ebene) – Verlagern Sie die Infrastruktur in die Cloud, ohne neue Hardware kaufen, Anwendungen umschreiben oder Ihre bestehenden Abläufe ändern zu müssen. Sie migrieren Server von einer lokalen Plattform zu einem Cloud-Dienst für dieselbe Plattform. Beispiel: Migrieren Sie eine Microsoft Hyper-V Anwendung zu AWS.
- Beibehaltung (Wiederaufgreifen) – Bewahren Sie Anwendungen in Ihrer Quellumgebung auf. Dazu können Anwendungen gehören, die einen umfangreichen Faktorwechsel erfordern und

die Sie auf einen späteren Zeitpunkt verschieben möchten, sowie ältere Anwendungen, die Sie beibehalten möchten, da es keine geschäftliche Rechtfertigung für ihre Migration gibt.

- Außerbetriebnahme – Dekommissionierung oder Entfernung von Anwendungen, die in Ihrer Quellumgebung nicht mehr benötigt werden.

A

A2A () Agent-to-Agent

Ein Stateful-Protokoll für die Zusammenarbeit zwischen Agenten, das die Delegierung von Aufgaben und die Zustandsübertragung unterstützt.

ABAC

Siehe attributbasierte Zugriffskontrolle.

abstrahierte Dienste

Siehe Managed Services.

ACID

Siehe Atomarität, Konsistenz, Isolierung und Haltbarkeit.

Aktiv-Aktiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden (mithilfe eines bidirektionalen Replikationstools oder dualer Schreibvorgänge) und beide Datenbanken Transaktionen von miteinander verbundenen Anwendungen während der Migration verarbeiten. Diese Methode unterstützt die Migration in kleinen, kontrollierten Batches, anstatt einen einmaligen Cutover zu erfordern. Es ist flexibler, erfordert aber mehr Arbeit als eine aktiv-passive Migration.

Aktiv-Passiv-Migration

Eine Datenbankmigrationsmethode, bei der die Quell- und Zieldatenbanken synchron gehalten werden, aber nur die Quelldatenbank verarbeitet Transaktionen von verbindenden Anwendungen, während Daten in die Zieldatenbank repliziert werden. Die Zieldatenbank akzeptiert während der Migration keine Transaktionen.

Agent

Ein KI-System, das mithilfe von Tools selbständig Überlegungen anstellen, planen und Maßnahmen ergreifen kann, um Ziele zu erreichen.

Agent Ops

Operative Verfahren zum Erstellen, Testen, Bereitstellen und Ausführen von KI-Agenten in der Produktion im großen Maßstab.

Aggregatfunktion

Eine SQL-Funktion, die mit einer Gruppe von Zeilen arbeitet und einen einzelnen Rückgabewert für die Gruppe berechnet. Beispiele für Aggregatfunktionen sind `SUM` und`MAX`.

AI

Siehe künstliche Intelligenz.

AIOps

Siehe Operationen mit künstlicher Intelligenz.

Anonymisierung

Der Prozess des dauerhaften Löschens personenbezogener Daten in einem Datensatz. Anonymisierung kann zum Schutz der Privatsphäre beitragen. Anonymisierte Daten gelten nicht mehr als personenbezogene Daten.

Anti-Muster

Eine häufig verwendete Lösung für ein wiederkehrendes Problem, bei dem die Lösung kontraproduktiv, ineffektiv oder weniger wirksam als eine Alternative ist.

Anwendungssteuerung

Ein Sicherheitsansatz, bei dem nur zugelassene Anwendungen verwendet werden können, um ein System vor Schadsoftware zu schützen.

Anwendungsportfolio

Eine Sammlung detaillierter Informationen zu jeder Anwendung, die von einer Organisation verwendet wird, einschließlich der Kosten für die Erstellung und Wartung der Anwendung und ihres Geschäftswerts. Diese Informationen sind entscheidend für den Prozess der Portfoliofindung und -analyse und hilft bei der Identifizierung und Priorisierung der Anwendungen, die migriert, modernisiert und optimiert werden sollen.

künstliche Intelligenz (KI)

Das Gebiet der Datenverarbeitungswissenschaft, das sich der Nutzung von Computertechnologien zur Ausführung kognitiver Funktionen widmet, die typischerweise mit

Menschen in Verbindung gebracht werden, wie Lernen, Problemlösen und Erkennen von Mustern. Weitere Informationen finden Sie unter Was ist künstliche Intelligenz?

Operationen mit künstlicher Intelligenz (AIOps)

Der Prozess des Einsatzes von Techniken des Machine Learning zur Lösung betrieblicher Probleme, zur Reduzierung betrieblicher Zwischenfälle und menschlicher Eingriffe sowie zur Steigerung der Servicequalität. Weitere Informationen zur Verwendung von AIOps in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Betriebsintegration.

Asymmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der ein Schlüsselpaar, einen öffentlichen Schlüssel für die Verschlüsselung und einen privaten Schlüssel für die Entschlüsselung verwendet. Sie können den öffentlichen Schlüssel teilen, da er nicht für die Entschlüsselung verwendet wird. Der Zugriff auf den privaten Schlüssel sollte jedoch stark eingeschränkt sein.

Atomizität, Konsistenz, Isolierung, Haltbarkeit (ACID)

Eine Reihe von Softwareeigenschaften, die die Datenvalidität und betriebliche Zuverlässigkeit einer Datenbank auch bei Fehlern, Stromausfällen oder anderen Problemen gewährleisten.

Attributbasierte Zugriffskontrolle (ABAC)

Die Praxis, detaillierte Berechtigungen auf der Grundlage von Benutzerattributen wie Abteilung, Aufgabenrolle und Teamname zu erstellen. Weitere Informationen finden Sie unter ABAC AWS in der AWS Identity and Access Management (IAM-) Dokumentation.

autoritative Datenquelle

Ein Ort, an dem Sie die primäre Version der Daten speichern, die als die zuverlässigste Informationsquelle angesehen wird. Sie können Daten aus der maßgeblichen Datenquelle an andere Speicherorte kopieren, um die Daten zu verarbeiten oder zu ändern, z. B. zu anonymisieren, zu redigieren oder zu pseudonymisieren.

Availability Zone

Ein bestimmter Standort innerhalb einer AWS-Region , der vor Ausfällen in anderen Availability Zones geschützt ist und kostengünstige Netzwerkkonnektivität mit niedriger Latenz zu anderen Availability Zones in derselben Region bietet.

AWS Framework für die Einführung der Cloud (AWS CAF)

Ein Framework mit Richtlinien und bewährten Verfahren, das Unternehmen bei der Entwicklung eines effizienten und effektiven Plans für den erfolgreichen Umstieg auf die Cloud unterstützt.

AWS AWS CAF unterteilt die Leitlinien in sechs Schwerpunktbereiche, die als Perspektiven bezeichnet werden: Unternehmen, Mitarbeiter, Unternehmensführung, Plattform, Sicherheit und Betrieb. Die Perspektiven Geschäft, Mitarbeiter und Unternehmensführung konzentrieren sich auf Geschäftskompetenzen und -prozesse, während sich die Perspektiven Plattform, Sicherheit und Betriebsabläufe auf technische Fähigkeiten und Prozesse konzentrieren. Die Personalperspektive zielt beispielsweise auf Stakeholder ab, die sich mit Personalwesen (HR), Personalfunktionen und Personalmanagement befassen. Aus dieser Perspektive bietet AWS CAF Leitlinien für Personalentwicklung, Schulung und Kommunikation, um das Unternehmen auf eine erfolgreiche Cloud-Einführung vorzubereiten. Weitere Informationen finden Sie auf der AWS -CAF-Webseite und dem AWS -CAF-Whitepaper.

AWS Workload-Qualifizierungsrahmen (AWS WQF)

Ein Tool, das Workloads bei der Datenbankmigration bewertet, Migrationsstrategien empfiehlt und Arbeitsschätzungen bereitstellt. AWS WQF ist in () enthalten. AWS Schema Conversion Tool AWS SCT Es analysiert Datenbankschemas und Codeobjekte, Anwendungscode, Abhängigkeiten und Leistungsmerkmale und stellt Bewertungsberichte bereit.

B

schlechter Bot

Ein Bot, der Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen soll.

BCP

Siehe Planung der Geschäftskontinuität.

Verhaltensdiagramm

Eine einheitliche, interaktive Ansicht des Ressourcenverhaltens und der Interaktionen im Laufe der Zeit. Sie können ein Verhaltensdiagramm mit Amazon Detective verwenden, um fehlgeschlagene Anmeldeversuche, verdächtige API-Aufrufe und ähnliche Vorgänge zu untersuchen. Weitere Informationen finden Sie unter Daten in einem Verhaltensdiagramm in der Detective-Dokumentation.

Big-Endian-System

Ein System, welches das höchstwertige Byte zuerst speichert. Siehe auch Endianness.

Binäre Klassifikation

Ein Prozess, der ein binäres Ergebnis vorhersagt (eine von zwei möglichen Klassen). Beispielsweise könnte Ihr ML-Modell möglicherweise Probleme wie „Handelt es sich bei dieser E-Mail um Spam oder nicht?“ vorhersagen müssen oder „Ist dieses Produkt ein Buch oder ein Auto?“

Bloom-Filter

Eine probabilistische, speichereffiziente Datenstruktur, mit der getestet wird, ob ein Element Teil einer Menge ist.

blue/green Einsatz

Eine Bereitstellungsstrategie, bei der Sie zwei separate, aber identische Umgebungen erstellen. Sie führen die aktuelle Anwendungsversion in einer Umgebung (blau) und die neue Anwendungsversion in der anderen Umgebung (grün) aus. Mit dieser Strategie können Sie schnell und mit minimalen Auswirkungen ein Rollback durchführen.

Bot

Eine Softwareanwendung, die automatisierte Aufgaben über das Internet ausführt und menschliche Aktivitäten oder Interaktionen simuliert. Manche Bots sind nützlich oder nützlich, wie z. B. Webcrawler, die Informationen im Internet indexieren. Einige andere Bots, sogenannte bösartige Bots, sollen Einzelpersonen oder Organisationen stören oder ihnen Schaden zufügen.

Botnetz

Netzwerke von Bots, die mit Malware infiziert sind und unter der Kontrolle einer einzigen Partei stehen, die als Bot-Herder oder Bot-Operator bezeichnet wird. Botnetze sind der bekannteste Mechanismus zur Skalierung von Bots und ihrer Wirkung.

branch

Ein containerisierter Bereich eines Code-Repositorys. Der erste Zweig, der in einem Repository erstellt wurde, ist der Hauptzweig. Sie können einen neuen Zweig aus einem vorhandenen Zweig erstellen und dann Feature entwickeln oder Fehler in dem neuen Zweig beheben. Ein Zweig, den Sie erstellen, um ein Feature zu erstellen, wird allgemein als Feature-Zweig bezeichnet. Wenn das Feature zur Veröffentlichung bereit ist, führen Sie den Feature-Zweig wieder mit dem Hauptzweig zusammen. Weitere Informationen finden Sie unter Über Branches (GitHub Dokumentation).

Zugang durch Glasbruch

Unter außergewöhnlichen Umständen und im Rahmen eines genehmigten Verfahrens ist dies eine schnelle Methode für einen Benutzer, auf einen Bereich zuzugreifen AWS-Konto , für den er in der Regel keine Zugriffsrechte besitzt. Weitere Informationen finden Sie in den Leitlinien unter dem Indikator „Glasbruchverfahren implementieren“. AWS Well-Architected

Brownfield-Strategie

Die bestehende Infrastruktur in Ihrer Umgebung. Wenn Sie eine Brownfield-Strategie für eine Systemarchitektur anwenden, richten Sie sich bei der Gestaltung der Architektur nach den Einschränkungen der aktuellen Systeme und Infrastruktur. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Puffer-Cache

Der Speicherbereich, in dem die am häufigsten abgerufenen Daten gespeichert werden.

Geschäftsfähigkeit

Was ein Unternehmen tut, um Wert zu generieren (z. B. Vertrieb, Kundenservice oder Marketing). Microservices-Architekturen und Entwicklungsentscheidungen können von den Geschäftskapazitäten beeinflusst werden. Weitere Informationen finden Sie im Abschnitt Organisiert nach Geschäftskapazitäten des Whitepapers Ausführen von containerisierten Microservices in AWS.

Planung der Geschäftskontinuität (BCP)

Ein Plan, der die potenziellen Auswirkungen eines störenden Ereignisses, wie z. B. einer groß angelegten Migration, auf den Betrieb berücksichtigt und es einem Unternehmen ermöglicht, den Betrieb schnell wieder aufzunehmen.

C

CAF

Weitere Informationen finden Sie unter AWS Framework für die Cloud-Einführung.

Bereitstellung auf Kanaren

Die langsame und schrittweise Veröffentlichung einer Version für Endbenutzer. Wenn Sie sich sicher sind, stellen Sie die neue Version bereit und ersetzen die aktuelle Version vollständig.

CCoE

Weitere Informationen finden Sie im Cloud Center of Excellence.

CDC

Siehe Erfassung von Änderungsdaten.

Erfassung von Datenänderungen (CDC)

Der Prozess der Nachverfolgung von Änderungen an einer Datenquelle, z. B. einer Datenbanktabelle, und der Aufzeichnung von Metadaten zu der Änderung. Sie können CDC für verschiedene Zwecke verwenden, z. B. für die Prüfung oder Replikation von Änderungen in einem Zielsystem, um die Synchronisation aufrechtzuerhalten.

Chaos-Technik

Absichtliches Einführen von Ausfällen oder Störungsereignissen, um die Widerstandsfähigkeit eines Systems zu testen. Sie können AWS Fault Injection Service (AWS FIS) verwenden, um Experimente durchzuführen, die Ihre AWS Workloads stress, und deren Reaktion zu bewerten.

CI/CD

Siehe Continuous Integration und Continuous Delivery.

Klassifizierung

Ein Kategorisierungsprozess, der bei der Erstellung von Vorhersagen hilft. ML-Modelle für Klassifikationsprobleme sagen einen diskreten Wert voraus. Diskrete Werte unterscheiden sich immer voneinander. Beispielsweise muss ein Modell möglicherweise auswerten, ob auf einem Bild ein Auto zu sehen ist oder nicht.

Citizen Developer

Ein Geschäftsanwender, der KI-Anwendungen mithilfe von Plattformen ohne Programmierkenntnisse erstellt. code/low

clientseitige Verschlüsselung

Lokale Verschlüsselung von Daten, bevor das Ziel sie AWS-Service empfängt.

Cloud-Kompetenzzentrum (CCoE)

Ein multidisziplinäres Team, das die Cloud-Einführung in der gesamten Organisation vorantreibt, einschließlich der Entwicklung bewährter Cloud-Methoden, der Mobilisierung von Ressourcen, der Festlegung von Migrationszeitplänen und der Begleitung der Organisation durch groß angelegte

Transformationen. Weitere Informationen finden Sie in den CCoE-Beiträgen im AWS Cloud Enterprise Strategy Blog.

Cloud Computing

Die Cloud-Technologie, die typischerweise für die Ferndatenspeicherung und das IoT-Gerätemanagement verwendet wird. Cloud Computing ist häufig mit Edge-Computing-Technologie verbunden.

Cloud-Betriebsmodell

In einer IT-Organisation das Betriebsmodell, das zum Aufbau, zur Weiterentwicklung und Optimierung einer oder mehrerer Cloud-Umgebungen verwendet wird. Weitere Informationen finden Sie unter Aufbau Ihres Cloud-Betriebsmodells.

Phasen der Einführung der Cloud

Die vier Phasen, die Unternehmen bei der Migration in der Regel durchlaufen AWS Cloud:

- Projekt – Durchführung einiger Cloud-bezogener Projekte zu Machbarkeitsnachweisen und zu Lernzwecken
- Fundament – Grundlegende Investitionen tätigen, um Ihre Cloud-Einführung zu skalieren (z. B. Einrichtung einer Landing Zone, Definition eines CCoE, Einrichtung eines Betriebsmodells)
- Migration – Migrieren einzelner Anwendungen
- Re-invention — Optimierung von Produkten und Dienstleistungen sowie Innovation in der Cloud

Diese Phasen wurden von Stephen Orban im Blogbeitrag The Journey Toward Cloud-First & the Stages of Adoption im AWS Cloud Enterprise Strategy-Blog definiert. Informationen darüber, wie sie mit der AWS Migrationsstrategie zusammenhängen, finden Sie im Leitfaden zur Vorbereitung der Migration.

CMDB

Siehe Datenbank für das Konfigurationsmanagement.

Code-Repository

Ein Ort, an dem Quellcode und andere Komponenten wie Dokumentation, Beispiele und Skripts gespeichert und im Rahmen von Versionskontrollprozessen aktualisiert werden. Zu den gängigen Cloud-Repositorys gehören GitHub oderBitbucket Cloud. Jede Version des Codes wird Zweig genannt. In einer Microservice-Struktur ist jedes Repository einer einzelnen Funktionalität gewidmet. Eine einzelne CI/CD Pipeline kann mehrere Repositorys verwenden.

Kalter Cache

Ein Puffer-Cache, der leer oder nicht gut gefüllt ist oder veraltete oder irrelevante Daten enthält. Dies beeinträchtigt die Leistung, da die Datenbank-Instance aus dem Hauptspeicher oder der Festplatte lesen muss, was langsamer ist als das Lesen aus dem Puffercache.

Kalte Daten

Daten, auf die selten zugegriffen wird und die in der Regel historisch sind. Bei der Abfrage dieser Art von Daten sind langsame Abfragen in der Regel akzeptabel. Durch die Verlagerung dieser Daten auf leistungsschwächere und kostengünstigere Speicherstufen oder -klassen können Kosten gesenkt werden.

Computer Vision (CV)

Ein Bereich der KI, der maschinelles Lernen nutzt, um Informationen aus visuellen Formaten wie digitalen Bildern und Videos zu analysieren und zu extrahieren. Amazon SageMaker AI bietet beispielsweise Bildverarbeitungsalgorithmen für CV.

Drift in der Konfiguration

Bei einer Arbeitslast eine Änderung der Konfiguration gegenüber dem erwarteten Zustand. Dies kann dazu führen, dass der Workload nicht mehr richtlinienkonform wird, und zwar in der Regel schrittweise und unbeabsichtigt.

Verwaltung der Datenbankkonfiguration (CMDB)

Ein Repository, das Informationen über eine Datenbank und ihre IT-Umgebung speichert und verwaltet, inklusive Hardware- und Softwarekomponenten und deren Konfigurationen. In der Regel verwenden Sie Daten aus einer CMDB in der Phase der Portfolioerkennung und -analyse der Migration.

Konformitätspaket

Eine Sammlung von AWS Config Regeln und Abhilfemaßnahmen, die Sie zusammenstellen können, um Ihre Konformitäts- und Sicherheitsprüfungen individuell anzupassen. Mithilfe einer YAML-Vorlage können Sie ein Conformance Pack als einzelne Entität in einer AWS-Konto AND-Region oder unternehmensweit bereitstellen. Weitere Informationen finden Sie in der Dokumentation unter Conformance Packs. AWS Config

kontinuierliche Integration und kontinuierliche Bereitstellung () CI/CD

Der Prozess der Automatisierung der Quell-, Build-, Test-, Staging- und Produktionsphasen des Softwareveröffentlichungsprozesses. CI/CD wird allgemein als Pipeline beschrieben. CI/CD

kann Ihnen helfen, Prozesse zu automatisieren, die Produktivität zu steigern, die Codequalität zu verbessern und schneller zu liefern. Weitere Informationen finden Sie unter Vorteile der kontinuierlichen Auslieferung. CD kann auch für kontinuierliche Bereitstellung stehen. Weitere Informationen finden Sie unterKontinuierliche Auslieferung im Vergleich zu kontinuierlicher Bereitstellung.

CV

Siehe Computer Vision.

D

Daten im Ruhezustand

Daten, die in Ihrem Netzwerk stationär sind, z. B. Daten, die sich im Speicher befinden.

Datenklassifizierung

Ein Prozess zur Identifizierung und Kategorisierung der Daten in Ihrem Netzwerk auf der Grundlage ihrer Kritikalität und Sensitivität. Sie ist eine wichtige Komponente jeder Strategie für das Management von Cybersecurity-Risiken, da sie Ihnen hilft, die geeigneten Schutz- und Aufbewahrungskontrollen für die Daten zu bestimmen. Die Datenklassifizierung ist ein Bestandteil der Sicherheitssäule des AWS Well-Architected Frameworks. Weitere Informationen finden Sie unter Datenklassifizierung.

Datendrift

Eine signifikante Variation zwischen den Produktionsdaten und den Daten, die zum Trainieren eines ML-Modells verwendet wurden, oder eine signifikante Änderung der Eingabedaten im Laufe der Zeit. Datendrift kann die Gesamtqualität, Genauigkeit und Fairness von ML-Modellvorhersagen beeinträchtigen.

Daten während der Übertragung

Daten, die sich aktiv durch Ihr Netzwerk bewegen, z. B. zwischen Netzwerkressourcen.

Datennetz

Ein architektonisches Framework, das verteilte, dezentrale Dateneigentum mit zentraler Verwaltung und Steuerung ermöglicht.

Datenminimierung

Das Prinzip, nur die Daten zu sammeln und zu verarbeiten, die unbedingt erforderlich sind. Durch Datenminimierung im AWS Cloud können Datenschutzrisiken, Kosten und der CO2-Fußabdruck Ihrer Analysen reduziert werden.

Datenperimeter

Eine Reihe präventiver Schutzmaßnahmen in Ihrer AWS Umgebung, die sicherstellen, dass nur vertrauenswürdige Identitäten auf vertrauenswürdige Ressourcen von erwarteten Netzwerken zugreifen. Weitere Informationen finden Sie unter Aufbau eines Datenperimeters auf. AWS

Vorverarbeitung der Daten

Rohdaten in ein Format umzuwandeln, das von Ihrem ML-Modell problemlos verarbeitet werden kann. Die Vorverarbeitung von Daten kann bedeuten, dass bestimmte Spalten oder Zeilen entfernt und fehlende, inkonsistente oder doppelte Werte behoben werden.

Herkunft der Daten

Der Prozess der Nachverfolgung des Ursprungs und der Geschichte von Daten während ihres gesamten Lebenszyklus, z. B. wie die Daten generiert, übertragen und gespeichert wurden.

betroffene Person

Eine Person, deren Daten gesammelt und verarbeitet werden.

Data Warehouse

Ein Datenverwaltungssystem, das Business Intelligence wie Analysen unterstützt. Data Warehouses enthalten in der Regel große Mengen historischer Daten und werden in der Regel für Abfragen und Analysen verwendet.

Datenbankdefinitionssprache (DDL)

Anweisungen oder Befehle zum Erstellen oder Ändern der Struktur von Tabellen und Objekten in einer Datenbank.

Datenbankmanipulationssprache (DML)

Anweisungen oder Befehle zum Ändern (Einfügen, Aktualisieren und Löschen) von Informationen in einer Datenbank.

DDL

Siehe Datenbankdefinitionssprache.

Deep-Ensemble

Mehrere Deep-Learning-Modelle zur Vorhersage kombinieren. Sie können Deep-Ensembles verwenden, um eine genauere Vorhersage zu erhalten oder um die Unsicherheit von Vorhersagen abzuschätzen.

Deep Learning

Ein ML-Teilbereich, der mehrere Schichten künstlicher neuronaler Netzwerke verwendet, um die Zuordnung zwischen Eingabedaten und Zielvariablen von Interesse zu ermitteln.

Tiefgreifende Verteidigung

Ein Ansatz zur Informationssicherheit, bei dem eine Reihe von Sicherheitsmechanismen und -kontrollen sorgfältig in einem Computernetzwerk verteilt werden, um die Vertraulichkeit, Integrität und Verfügbarkeit des Netzwerks und der darin enthaltenen Daten zu schützen. Wenn Sie diese Strategie anwenden AWS, fügen Sie mehrere Steuerelemente auf verschiedenen Ebenen der AWS Organizations Struktur hinzu, um die Ressourcen zu schützen. Ein umfassender Verteidigungsansatz könnte beispielsweise Multi-Faktor-Authentifizierung, Netzwerksegmentierung und Verschlüsselung kombinieren.

delegierter Administrator

In kann ein kompatibler Dienst ein AWS Mitgliedskonto registrieren AWS Organizations, um die Konten der Organisation zu verwalten und die Berechtigungen für diesen Dienst zu verwalten. Dieses Konto wird als delegierter Administrator für diesen Service bezeichnet. Weitere Informationen und eine Liste kompatibler Services finden Sie unter Services, die mit AWS Organizations funktionieren in der AWS Organizations -Dokumentation.

Einsatz

Der Prozess, bei dem eine Anwendung, neue Feature oder Codekorrekturen in der Zielumgebung verfügbar gemacht werden. Die Bereitstellung umfasst das Implementieren von Änderungen an einer Codebasis und das anschließende Erstellen und Ausführen dieser Codebasis in den Anwendungsumgebungen.

Entwicklungsumgebung

Siehe Umgebung.

Detektivische Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, ein Ereignis zu erkennen, zu protokollieren und zu warnen, nachdem ein Ereignis eingetreten ist. Diese Kontrollen stellen eine zweite Verteidigungslinie dar und warnen Sie vor Sicherheitsereignissen, bei denen die vorhandenen

präventiven Kontrollen umgangen wurden. Weitere Informationen finden Sie unter Detektivische Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Abbildung des Wertstroms in der Entwicklung (DVSM)

Ein Prozess zur Identifizierung und Priorisierung von Einschränkungen, die sich negativ auf Geschwindigkeit und Qualität im Lebenszyklus der Softwareentwicklung auswirken. DVSM erweitert den Prozess der Wertstromanalyse, der ursprünglich für Lean-Manufacturing-Praktiken konzipiert wurde. Es konzentriert sich auf die Schritte und Teams, die erforderlich sind, um durch den Softwareentwicklungsprozess Mehrwert zu schaffen und zu steigern.

digitaler Zwilling

Eine virtuelle Darstellung eines realen Systems, z. B. eines Gebäudes, einer Fabrik, einer Industrieanlage oder einer Produktionslinie. Digitale Zwillinge unterstützen vorausschauende Wartung, Fernüberwachung und Produktionsoptimierung.

Maßtabelle

In einem Sternschema eine kleinere Tabelle, die Datenattribute zu quantitativen Daten in einer Faktentabelle enthält. Bei Attributen von Dimensionstabellen handelt es sich in der Regel um Textfelder oder diskrete Zahlen, die sich wie Text verhalten. Diese Attribute werden häufig zum Einschränken von Abfragen, zum Filtern und zur Kennzeichnung von Ergebnismengen verwendet.

Katastrophe

Ein Ereignis, das verhindert, dass ein Workload oder ein System seine Geschäftsziele an seinem primären Einsatzort erfüllt. Diese Ereignisse können Naturkatastrophen, technische Ausfälle oder das Ergebnis menschlichen Handelns sein, z. B. unbeabsichtigte Fehlkonfigurationen oder ein Malware-Angriff.

Disaster Recovery (DR)

Die Strategie und der Prozess, die Sie zur Minimierung von Ausfallzeiten und Datenverlusten aufgrund einer Katastrophe anwenden. Weitere Informationen finden Sie unter Disaster Recovery von Workloads unter AWS: Wiederherstellung in der Cloud im AWS Well-Architected Framework.

DML

Siehe Sprache zur Datenbankmanipulation.

Domainorientiertes Design

Ein Ansatz zur Entwicklung eines komplexen Softwaresystems, bei dem seine Komponenten mit sich entwickelnden Domains oder Kerngeschäftszielen verknüpft werden, denen jede

Komponente dient. Dieses Konzept wurde von Eric Evans in seinem Buch Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003) vorgestellt. Informationen darüber, wie Sie domänengesteuertes Design mit dem Strangler-Fig-Muster verwenden können, finden Sie unter Schrittweise Modernisierung älterer Microsoft ASP.NET (ASMX) -Webservices mithilfe von Containern und Amazon API Gateway.

DR

Siehe Disaster Recovery.

Erkennung von Driften

Verfolgung von Abweichungen von einer Basiskonfiguration Sie können es beispielsweise verwenden, AWS CloudFormation um Abweichungen bei den Systemressourcen zu erkennen, oder Sie können AWS Control Tower damit Änderungen in Ihrer landing zone erkennen, die sich auf die Einhaltung von Governance-Anforderungen auswirken könnten.

DVSM

Siehe Abbildung der Wertströme in der Entwicklung.

E

EDA

Siehe explorative Datenanalyse.

EDI

Siehe elektronischer Datenaustausch.

Edge-Computing

Die Technologie, die die Rechenleistung für intelligente Geräte an den Rändern eines IoT-Netzwerks erhöht. Im Vergleich zu Cloud Computing kann Edge Computing die Kommunikationslatenz reduzieren und die Reaktionszeit verbessern.

elektronischer Datenaustausch (EDI)

Der automatisierte Austausch von Geschäftsdokumenten zwischen Organisationen. Weitere Informationen finden Sie unter Was ist elektronischer Datenaustausch.

Verschlüsselung

Ein Rechenprozess, der Klartextdaten, die für Menschen lesbar sind, in Chiffretext umwandelt.

Verschlüsselungsschlüssel

Eine kryptografische Zeichenfolge aus zufälligen Bits, die von einem Verschlüsselungsalgorithmus generiert wird. Schlüssel können unterschiedlich lang sein, und jeder Schlüssel ist so konzipiert, dass er unvorhersehbar und einzigartig ist.

Endianismus

Die Reihenfolge, in der Bytes im Computerspeicher gespeichert werden. Big-endian Systeme speichern das höchstwertige Byte zuerst. Little-endian Systeme speichern das niedrigstwertige Byte zuerst.

Endpunkt

Siehe Service-Endpunkt.

Endpunkt-Services

Ein Service, den Sie in einer Virtual Private Cloud (VPC) hosten können, um ihn mit anderen Benutzern zu teilen. Sie können einen Endpunktdienst mit anderen AWS-Konten oder AWS Identity and Access Management (IAM AWS PrivateLink -) Prinzipalen erstellen und diesen Berechtigungen gewähren. Diese Konten oder Prinzipale können sich privat mit Ihrem Endpunktservice verbinden, indem sie Schnittstellen-VPC-Endpunkte erstellen. Weitere Informationen finden Sie unter Einen Endpunkt-Service erstellen in der Amazon Virtual Private Cloud (Amazon VPC)-Dokumentation.

Unternehmensressourcenplanung (ERP)

Ein System, das wichtige Geschäftsprozesse (wie Buchhaltung, MES und Projektmanagement) für ein Unternehmen automatisiert und verwaltet.

Envelope-Verschlüsselung

Der Prozess der Verschlüsselung eines Verschlüsselungsschlüssels mit einem anderen Verschlüsselungsschlüssel. Weitere Informationen finden Sie unter Envelope-Verschlüsselung in der AWS Key Management Service (AWS KMS) -Dokumentation.

Umgebung

Eine Instance einer laufenden Anwendung. Die folgenden Arten von Umgebungen sind beim Cloud-Computing üblich:

- Entwicklungsumgebung – Eine Instance einer laufenden Anwendung, die nur dem Kernteam zur Verfügung steht, das für die Wartung der Anwendung verantwortlich ist. Entwicklungsumgebungen werden verwendet, um Änderungen zu testen, bevor sie in höhere

Umgebungen übertragen werden. Diese Art von Umgebung wird manchmal als Testumgebung bezeichnet.

- Niedrigere Umgebungen – Alle Entwicklungsumgebungen für eine Anwendung, z. B. solche, die für erste Builds und Tests verwendet wurden.
- Produktionsumgebung – Eine Instance einer laufenden Anwendung, auf die Endbenutzer zugreifen können. In einer CI/CD Pipeline ist die Produktionsumgebung die letzte Bereitstellungsumgebung.
- Höhere Umgebungen – Alle Umgebungen, auf die auch andere Benutzer als das Kernentwicklungsteam zugreifen können. Dies kann eine Produktionsumgebung, Vorproduktionsumgebungen und Umgebungen für Benutzerakzeptanztests umfassen.

Epics

In der agilen Methodik sind dies funktionale Kategorien, die Ihnen helfen, Ihre Arbeit zu organisieren und zu priorisieren. Epics bieten eine allgemeine Beschreibung der Anforderungen und Implementierungsaufgaben. Zu den Sicherheitsepen AWS von CAF gehören beispielsweise Identitäts- und Zugriffsmanagement, Detektivkontrollen, Infrastruktursicherheit, Datenschutz und Reaktion auf Vorfälle. Weitere Informationen zu Epics in der AWS -Migrationsstrategie finden Sie im Leitfaden zur Programm-Implementierung.

ERP

Siehe Enterprise Resource Planning.

Explorative Datenanalyse (EDA)

Der Prozess der Analyse eines Datensatzes, um seine Hauptmerkmale zu verstehen. Sie sammeln oder aggregieren Daten und führen dann erste Untersuchungen durch, um Muster zu finden, Anomalien zu erkennen und Annahmen zu überprüfen. EDA wird durchgeführt, indem zusammenfassende Statistiken berechnet und Datenvisualisierungen erstellt werden.

F

Faktentabelle

Die zentrale Tabelle in einem Sternschema. Sie speichert quantitative Daten über den Geschäftsbetrieb. In der Regel enthält eine Faktentabelle zwei Arten von Spalten: Spalten, die Kennzahlen enthalten, und Spalten, die einen Fremdschlüssel für eine Dimensionstabelle enthalten.

schnell scheitern

Eine Philosophie, die häufige und inkrementelle Tests verwendet, um den Entwicklungslebenszyklus zu verkürzen. Dies ist ein wichtiger Bestandteil eines agilen Ansatzes.

Grenze zur Fehlerisolierung

Dabei handelt es sich um eine Grenze AWS Cloud, z. B. eine Availability Zone AWS-Region, eine Steuerungsebene oder eine Datenebene, die die Auswirkungen eines Fehlers begrenzt und die Widerstandsfähigkeit von Workloads verbessert. Weitere Informationen finden Sie unter Grenzen zur AWS Fehlerisolierung.

Feature-Zweig

Siehe Zweig.

Features

Die Eingabedaten, die Sie verwenden, um eine Vorhersage zu treffen. In einem Fertigungskontext könnten Feature beispielsweise Bilder sein, die regelmäßig von der Fertigungslinie aus aufgenommen werden.

Bedeutung der Feature

Wie wichtig ein Feature für die Vorhersagen eines Modells ist. Dies wird in der Regel als numerischer Wert ausgedrückt, der mit verschiedenen Techniken wie Shapley Additive Explanations (SHAP) und integrierten Gradienten berechnet werden kann. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit AWS.

Featuretransformation

Daten für den ML-Prozess optimieren, einschließlich der Anreicherung von Daten mit zusätzlichen Quellen, der Skalierung von Werten oder der Extraktion mehrerer Informationssätze aus einem einzigen Datenfeld. Das ermöglicht dem ML-Modell, von den Daten profitieren. Wenn Sie beispielsweise das Datum „27.05.2021 00:15:37“ in „2021“, „Mai“, „Donnerstag“ und „15“ aufschlüsseln, können Sie dem Lernalgorithmus helfen, nuancierte Muster zu erlernen, die mit verschiedenen Datenkomponenten verknüpft sind.

Eingabeaufforderung mit wenigen Klicks

Bereitstellung einer kleinen Anzahl von Beispielen, die die Aufgabe und das gewünschte Ergebnis veranschaulichen, bevor das LLM aufgefordert wird, eine ähnliche Aufgabe auszuführen. Bei dieser Technik handelt es sich um eine Anwendung des kontextbezogenen Lernens,

bei der Modelle anhand von Beispielen (Aufnahmen) lernen, die in Eingabeaufforderungen eingebettet sind. Few-shot Eingabeaufforderungen können bei Aufgaben, die spezifische Formatierungs-, Argumentations- oder Fachkenntnisse erfordern, effektiv sein. Siehe auch Zero-Shot-Eingabeaufforderung.

FGAC

Siehe detaillierte Zugriffskontrolle.

Feinkörnige Zugriffskontrolle (FGAC)

Die Verwendung mehrerer Bedingungen, um eine Zugriffsanfrage zuzulassen oder abzulehnen.

Flash-Cut-Migration

Eine Datenbankmigrationsmethode, bei der eine kontinuierliche Datenreplikation durch Erfassung von Änderungsdaten verwendet wird, um Daten in kürzester Zeit zu migrieren, anstatt einen schrittweisen Ansatz zu verwenden. Ziel ist es, Ausfallzeiten auf ein Minimum zu beschränken.

FM

Siehe Fundamentmodell.

Fundamentmodell (FM)

Ein großes neuronales Deep-Learning-Netzwerk, das mit riesigen Datensätzen generalisierter und unbeschrifteter Daten trainiert wurde. FMs sind in der Lage, eine Vielzahl allgemeiner Aufgaben zu erfüllen, z. B. Sprache zu verstehen, Text und Bilder zu generieren und Konversationen in natürlicher Sprache zu führen. Weitere Informationen finden Sie unter Was sind Foundation-Modelle.

FM-Gateway

Ein zentraler Vermittler, der den Zugriff auf Basismodelle kontrolliert und normalisiert. Wird auch als LLM-Gateway bezeichnet.

G

Generative KI

Eine Untergruppe von KI-Modellen, die mit großen Datenmengen trainiert wurden und mithilfe einer einfachen Textaufforderung neue Inhalte und Artefakte wie Bilder, Videos, Text und Audio erstellen können. Weitere Informationen finden Sie unter Was ist Generative KI.

Geoblocking

Siehe geografische Einschränkungen.

Geografische Einschränkungen (Geoblocking)

Bei Amazon eine Option CloudFront, um zu verhindern, dass Benutzer in bestimmten Ländern auf Inhaltsverteilungen zugreifen. Sie können eine Zulassungsliste oder eine Sperrliste verwenden, um zugelassene und gesperrte Länder anzugeben. Weitere Informationen finden Sie in der Dokumentation unter Beschränkung der geografischen Verteilung Ihrer Inhalte. CloudFront

Gitflow-Workflow

Ein Ansatz, bei dem niedrigere und höhere Umgebungen unterschiedliche Zweige in einem Quellcode-Repository verwenden. Der Gitflow-Workflow gilt als veraltet, und der Trunk-basierte Workflow ist der moderne, bevorzugte Ansatz.

goldenes Bild

Ein Snapshot eines Systems oder einer Software, der als Vorlage für die Bereitstellung neuer Instanzen dieses Systems oder dieser Software verwendet wird. In der Fertigung kann ein Golden Image beispielsweise zur Bereitstellung von Software auf mehreren Geräten verwendet werden und trägt so zur Verbesserung der Geschwindigkeit, Skalierbarkeit und Produktivität bei der Geräteherstellung bei.

Greenfield-Strategie

Das Fehlen vorhandener Infrastruktur in einer neuen Umgebung. Bei der Einführung einer Neuausrichtung einer Systemarchitektur können Sie alle neuen Technologien ohne Einschränkung der Kompatibilität mit der vorhandenen Infrastruktur auswählen, auch bekannt als Brownfield. Wenn Sie die bestehende Infrastruktur erweitern, könnten Sie Brownfield- und Greenfield-Strategien mischen.

Integritätsschutz

Eine allgemeine Regel, die dabei hilft, Ressourcen, Richtlinien und die Einhaltung von Vorschriften in allen Organisationseinheiten (OUs) zu regeln. Präventiver Integritätsschutz setzt Richtlinien durch, um die Einhaltung von Standards zu gewährleisten. Sie werden mithilfe von Service-Kontrollrichtlinien und IAM-Berechtigungsgrenzen implementiert. Detektivischer Integritätsschutz erkennt Richtlinienverstöße und Compliance-Probleme und generiert Warnmeldungen zur Abhilfe. Sie werden mithilfe von AWS Config, AWS Security Hub CSPM, Amazon GuardDuty AWS Trusted Advisor, Amazon Inspector und benutzerdefinierten AWS Lambda Prüfungen implementiert.

Leitplanken (KI)

Sicherheitsmechanismen, die Eingaben und Ausgaben von Agenten filtern, validieren und einschränken, um ein verantwortungsbewusstes und sicheres Verhalten der KI zu gewährleisten.

H

HEKTAR

Siehe Hochverfügbarkeit.

Heterogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank in eine Zieldatenbank, die eine andere Datenbank-Engine verwendet (z. B. Oracle zu Amazon Aurora). Eine heterogene Migration ist in der Regel Teil einer Neuarchitektur, und die Konvertierung des Schemas kann eine komplexe Aufgabe sein. AWS bietet AWS SCT, welches bei Schemakonvertierungen hilft.

hohe Verfügbarkeit (HA)

Die Fähigkeit eines Workloads, im Falle von Herausforderungen oder Katastrophen kontinuierlich und ohne Eingreifen zu arbeiten. HA-Systeme sind so konzipiert, dass sie automatisch ein Failover durchführen, gleichbleibend hohe Leistung bieten und unterschiedliche Lasten und Ausfälle mit minimalen Leistungseinbußen bewältigen.

historische Modernisierung

Ein Ansatz zur Modernisierung und Aufrüstung von Betriebstechnologiesystemen (OT), um den Bedürfnissen der Fertigungsindustrie besser gerecht zu werden. Ein Historian ist eine Art von Datenbank, die verwendet wird, um Daten aus verschiedenen Quellen in einer Fabrik zu sammeln und zu speichern.

Holdout-Daten

Ein Teil historischer, beschrifteter Daten, der aus einem Datensatz zurückgehalten wird, der zum Trainieren eines Modells für maschinelles Lernen verwendet wird. Sie können Holdout-Daten verwenden, um die Modellleistung zu bewerten, indem Sie die Modellvorhersagen mit den Holdout-Daten vergleichen.

Der Mensch im Kreis (HiTL)

Ein Workflow-Muster, bei dem die Ausführung von Agenten an kritischen Entscheidungspunkten unterbrochen wird, um von einem Mitarbeiter geprüft und genehmigt zu werden.

Homogene Datenbankmigration

Migrieren Sie Ihre Quelldatenbank zu einer Zieldatenbank, die dieselbe Datenbank-Engine verwendet (z. B. Microsoft SQL Server zu Amazon RDS für SQL Server). Eine homogene Migration ist in der Regel Teil eines Hostwechsels oder eines Plattformwechsels. Sie können native Datenbankserviceprogramme verwenden, um das Schema zu migrieren.

heiße Daten

Daten, auf die häufig zugegriffen wird, z. B. Echtzeitdaten oder aktuelle Translationsdaten. Für diese Daten ist in der Regel eine leistungsstarke Speicherebene oder -klasse erforderlich, um schnelle Abfrageantworten zu ermöglichen.

Hotfix

Eine dringende Lösung für ein kritisches Problem in einer Produktionsumgebung. Aufgrund seiner Dringlichkeit wird ein Hotfix normalerweise außerhalb des typischen DevOps Release-Workflows erstellt.

Hypercare-Phase

Unmittelbar nach dem Cutover, der Zeitraum, in dem ein Migrationsteam die migrierten Anwendungen in der Cloud verwaltet und überwacht, um etwaige Probleme zu beheben. In der Regel dauert dieser Zeitraum 1–4 Tage. Am Ende der Hypercare-Phase überträgt das Migrationsteam in der Regel die Verantwortung für die Anwendungen an das Cloud-Betriebsteam.

I

IaC

Sehen Sie sich Infrastruktur als Code an.

Identitätsbasierte Richtlinie

Eine Richtlinie, die einem oder mehreren IAM-Prinzipalen zugeordnet ist und deren Berechtigungen innerhalb der AWS Cloud Umgebung definiert.

Leerlaufanwendung

Eine Anwendung mit einer durchschnittlichen CPU- und Arbeitsspeicherauslastung zwischen 5 und 20 Prozent über einen Zeitraum von 90 Tagen. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen oder sie On-Premises beizubehalten.

IIoT

Siehe Industrielles Internet der Dinge.

unveränderliche Infrastruktur

Ein Modell, das eine neue Infrastruktur für Produktionsworkloads bereitstellt, anstatt die bestehende Infrastruktur zu aktualisieren, zu patchen oder zu modifizieren. Unveränderliche Infrastrukturen sind von Natur aus konsistenter, zuverlässiger und vorhersehbarer als veränderliche Infrastrukturen. Weitere Informationen finden Sie in der Best Practice Deploy using immutable infrastructure im Framework. AWS Well-Architected

Eingehende (ingress) VPC

In einer Architektur AWS mit mehreren Konten ist dies eine VPC, die Netzwerkverbindungen von außerhalb einer Anwendung akzeptiert, überprüft und weiterleitet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Inkrementelle Migration

Eine Cutover-Strategie, bei der Sie Ihre Anwendung in kleinen Teilen migrieren, anstatt eine einziges vollständiges Cutover durchzuführen. Beispielsweise könnten Sie zunächst nur einige Microservices oder Benutzer auf das neue System umstellen. Nachdem Sie sich vergewissert haben, dass alles ordnungsgemäß funktioniert, können Sie weitere Microservices oder Benutzer schrittweise verschieben, bis Sie Ihr Legacy-System außer Betrieb nehmen können. Diese Strategie reduziert die mit großen Migrationen verbundenen Risiken.

Industrie 4.0

Ein Begriff, der 2016 von Klaus Schwab eingeführt wurde und sich auf die Modernisierung von Fertigungsprozessen durch Fortschritte in den Bereichen Konnektivität, Echtzeitdaten, Automatisierung, Analytik und bezieht. AI/ML

Infrastruktur

Alle Ressourcen und Komponenten, die in der Umgebung einer Anwendung enthalten sind.

Infrastructure as Code (IaC)

Der Prozess der Bereitstellung und Verwaltung der Infrastruktur einer Anwendung mithilfe einer Reihe von Konfigurationsdateien. IaC soll Ihnen helfen, das Infrastrukturmanagement zu zentralisieren, Ressourcen zu standardisieren und schnell zu skalieren, sodass neue Umgebungen wiederholbar, zuverlässig und konsistent sind.

Industrielles Internet der Dinge (IIoT)

Einsatz von mit dem Internet verbundenen Sensoren und Geräten in Industriesektoren wie Fertigung, Energie, Automobilindustrie, Gesundheitswesen, Biowissenschaften und Landwirtschaft. Mehr Informationen finden Sie unter Aufbau einer digitalen Transformationsstrategie für das industrielle Internet der Dinge (IIoT).

Inspektions-VPC

In einer Architektur AWS mit mehreren Konten eine zentralisierte VPC, die Inspektionen des Netzwerkverkehrs zwischen VPCs (in derselben oder unterschiedlichen AWS-Regionen), dem Internet und lokalen Netzwerken verwaltet. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

Internet of Things (IoT)

Das Netzwerk verbundener physischer Objekte mit eingebetteten Sensoren oder Prozessoren, das über das Internet oder über ein lokales Kommunikationsnetzwerk mit anderen Geräten und Systemen kommuniziert. Weitere Informationen finden Sie unter Was ist IoT?

Interpretierbarkeit

Ein Merkmal eines Modells für Machine Learning, das beschreibt, inwieweit ein Mensch verstehen kann, wie die Vorhersagen des Modells von seinen Eingaben abhängen. Weitere Informationen finden Sie unter Interpretierbarkeit von Modellen für maschinelles Lernen mit. AWS

IoT

Siehe Internet der Dinge.

IT information library (ITIL, IT-Informationsbibliothek)

Eine Reihe von bewährten Methoden für die Bereitstellung von IT-Services und die Abstimmung dieser Services auf die Geschäftsanforderungen. ITIL bietet die Grundlage für ITSM.

T service management (ITSM, IT-Servicemanagement)

Aktivitäten im Zusammenhang mit der Gestaltung, Implementierung, Verwaltung und Unterstützung von IT-Services für eine Organisation. Informationen zur Integration von Cloud-Vorgängen mit ITSM-Tools finden Sie im Leitfaden zur Betriebsintegration.

BIS

Siehe IT-Informationsbibliothek.

ITSM

Siehe IT-Servicemanagement.

L

Labelbasierte Zugangskontrolle (LBAC)

Eine Implementierung der Mandatory Access Control (MAC), bei der den Benutzern und den Daten selbst jeweils explizit ein Sicherheitslabelwert zugewiesen wird. Die Schnittmenge zwischen der Benutzersicherheitsbeschriftung und der Datensicherheitsbeschriftung bestimmt, welche Zeilen und Spalten für den Benutzer sichtbar sind.

Landing Zone

Eine landing zone ist eine gut strukturierte AWS Umgebung mit mehreren Konten, die skalierbar und sicher ist. Dies ist ein Ausgangspunkt, von dem aus Ihre Organisationen Workloads und Anwendungen schnell und mit Vertrauen in ihre Sicherheits- und Infrastrukturumgebung starten und bereitstellen können. Weitere Informationen zu Landing Zones finden Sie unter Einrichtung einer sicheren und skalierbaren AWS -Umgebung mit mehreren Konten..

großes Sprachmodell (LLM)

Ein Deep-Learning-KI-Modell, das anhand einer riesigen Datenmenge vorab trainiert wurde. Ein LLM kann mehrere Aufgaben ausführen, z. B. Fragen beantworten, Dokumente zusammenfassen, Text in andere Sprachen übersetzen und Sätze vervollständigen. Weitere Informationen finden Sie unter Was sind LLMs.

Große Migration

Eine Migration von 300 oder mehr Servern.

LBAC

Siehe Labelbasierte Zugriffskontrolle.

Geringste Berechtigung

Die bewährte Sicherheitsmethode, bei der nur die für die Durchführung einer Aufgabe erforderlichen Mindestberechtigungen erteilt werden. Weitere Informationen finden Sie unter Geringste Berechtigungen anwenden in der IAM-Dokumentation.

Lift and Shift

Siehe 7 Rs.

Little-Endian-System

Ein System, welches das niedrigwertigste Byte zuerst speichert. Siehe auch Endianness.

LLM

Siehe großes Sprachmodell.

Niedrigere Umgebungen

Siehe Umgebung.

M

Machine Learning (ML)

Eine Art künstlicher Intelligenz, die Algorithmen und Techniken zur Mustererkennung und zum Lernen verwendet. ML analysiert aufgezeichnete Daten, wie z. B. Daten aus dem Internet der Dinge (IoT), und lernt daraus, um ein statistisches Modell auf der Grundlage von Mustern zu erstellen. Weitere Informationen finden Sie unter Machine Learning.

Hauptzweig

Siehe Filiale.

Malware

Software, die entwickelt wurde, um die Computersicherheit oder den Datenschutz zu gefährden. Malware kann Computersysteme stören, vertrauliche Informationen durchsickern lassen oder sich unbefugten Zugriff verschaffen. Beispiele für Malware sind Viren, Würmer, Ransomware, Trojaner, Spyware und Keylogger.

verwaltete Dienste

AWS-Services für die die Infrastrukturebene, das Betriebssystem und die Plattformen AWS betrieben werden, und Sie greifen auf die Endgeräte zu, um Daten zu speichern und abzurufen. Amazon Simple Storage Service (Amazon S3) und Amazon DynamoDB sind Beispiele für Managed Services. Diese werden auch als abstrakte Dienste bezeichnet.

Manufacturing Execution System (MES)

Ein Softwaresystem zur Verfolgung, Überwachung, Dokumentation und Steuerung von Produktionsprozessen, bei denen Rohstoffe in der Fertigung zu fertigen Produkten umgewandelt werden.

MAP

Siehe Migration Acceleration Program.

MCP

Siehe Model Context Protocol.

Model Context Protocol (MCP)

Ein zustandsloses Protokoll für die Kommunikation zwischen Agenten und Tool.

MCP-Server

Ein Dienst, der ein oder mehrere Tools über das Model Context Protocol verfügbar macht.

Mechanismus

Ein vollständiger Prozess, bei dem Sie ein Tool erstellen, die Akzeptanz des Tools vorantreiben und anschließend die Ergebnisse überprüfen, um Anpassungen vorzunehmen. Ein Mechanismus ist ein Zyklus, der sich im Laufe seiner Tätigkeit selbst verstärkt und verbessert. Weitere Informationen finden Sie unter Mechanismen im AWS Well-Architected Framework erstellen.

Mitgliedskonto

Alle AWS-Konten außer dem Verwaltungskonto, die Teil einer Organisation in sind AWS Organizations. Ein Konto kann jeweils nur Mitglied einer Organisation sein.

MES

Siehe Manufacturing Execution System.

Message Queuing-Telemetrietransport (MQTT)

Ein leichtes, auf dem publish/subscribeMuster basierendes M2M-Kommunikationsprotokoll (Machine-to-Machine) für IoT-Geräte mit beschränkten Ressourcen.

Microservice

Ein kleiner, unabhängiger Service, der über klar definierte APIs kommuniziert und in der Regel kleinen, eigenständigen Teams gehört. Ein Versicherungssystem kann beispielsweise Microservices beinhalten, die Geschäftsfunktionen wie Vertrieb oder Marketing oder Subdomains wie Einkauf, Schadenersatz oder Analytik zugeordnet sind. Zu den Vorteilen von Microservices gehören Agilität, flexible Skalierung, einfache Bereitstellung, wiederverwendbarer Code und Ausfallsicherheit. Weitere Informationen finden Sie unter Integration von Microservices mithilfe serverloser Dienste. AWS

Microservices-Architekturen

Ein Ansatz zur Erstellung einer Anwendung mit unabhängigen Komponenten, die jeden Anwendungsprozess als Microservice ausführen. Diese Microservices kommunizieren über eine klar definierte Schnittstelle mithilfe einfacher APIs. Jeder Microservice in dieser Architektur kann aktualisiert, bereitgestellt und skaliert werden, um den Bedarf an bestimmten Funktionen einer Anwendung zu decken. Weitere Informationen finden Sie unter Implementieren von Microservices auf. AWS

Migration Acceleration Program (MAP)

Ein AWS Programm, das Beratung, Unterstützung, Schulungen und Services bietet, um Unternehmen dabei zu unterstützen, eine solide betriebliche Grundlage für die Umstellung auf die Cloud zu schaffen und die anfänglichen Kosten von Migrationen auszugleichen. MAP umfasst eine Migrationsmethode für die methodische Durchführung von Legacy-Migrationen sowie eine Reihe von Tools zur Automatisierung und Beschleunigung gängiger Migrationsszenarien.

Migration in großem Maßstab

Der Prozess, bei dem der Großteil des Anwendungsportfolios in Wellen in die Cloud verlagert wird, wobei in jeder Welle mehr Anwendungen schneller migriert werden. In dieser Phase werden die bewährten Verfahren und Erkenntnisse aus den früheren Phasen zur Implementierung einer Migrationsfabrik von Teams, Tools und Prozessen zur Optimierung der Migration von Workloads durch Automatisierung und agile Bereitstellung verwendet. Dies ist die dritte Phase der AWS - Migrationsstrategie.

Migrationsfabrik

Cross-functional Teams, die die Migration von Workloads durch automatisierte, agile Ansätze optimieren. Zu den Teams von Migration Factory gehören in der Regel Betriebsanalysten und Eigentümer, Migrationsingenieure, Entwickler und DevOps Experten, die in Sprints arbeiten. Zwischen 20 und 50 Prozent eines Unternehmensanwendungsportfolios bestehen aus sich wiederholenden Mustern, die durch einen Fabrik-Ansatz optimiert werden können. Weitere Informationen finden Sie in Diskussion über Migrationsfabriken und den Leitfaden zur Cloud-Migration-Fabrik in diesem Inhaltssatz.

Migrationsmetadaten

Die Informationen über die Anwendung und den Server, die für den Abschluss der Migration benötigt werden. Für jedes Migrationsmuster ist ein anderer Satz von Migrationsmetadaten erforderlich. Beispiele für Migrationsmetadaten sind das Zielsubnetz, die Sicherheitsgruppe und AWS das Konto.

Migrationsmuster

Eine wiederholbare Migrationsaufgabe, in der die Migrationsstrategie, das Migrationsziel und die verwendete Migrationsanwendung oder der verwendete Migrationsservice detailliert beschrieben werden. Beispiel: Rehost-Migration zu Amazon EC2 mit AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Ein Online-Tool, das Informationen zur Validierung des Geschäftsszenarios für die Migration auf das bereitstellt. AWS Cloud MPA bietet eine detaillierte Portfoliobewertung (richtige Servergröße, Preisgestaltung, Gesamtbetriebskostenanalyse, Migrationskostenanalyse) sowie Migrationsplanung (Anwendungsdatenanalyse und Datenerfassung, Anwendungsgruppierung, Migrationspriorisierung und Wellenplanung). Das MPA-Tool (Anmeldung erforderlich) steht allen AWS Beratern und APN-Partnerberatern kostenlos zur Verfügung.

Migration Readiness Assessment (MRA)

Der Prozess, bei dem mithilfe des AWS CAF Erkenntnisse über den Cloud-Bereitschaftsstatus eines Unternehmens gewonnen, Stärken und Schwächen identifiziert und ein Aktionsplan zur Schließung festgestellter Lücken erstellt wird. Weitere Informationen finden Sie im Benutzerhandbuch für Migration Readiness. MRA ist die erste Phase der AWS - Migrationsstrategie.

Migrationsstrategie

Der Ansatz, der verwendet wurde, um einen Workload auf den AWS Cloud zu migrieren. Weitere Informationen finden Sie im Eintrag 7 Rs in diesem Glossar und unter Mobilisieren Sie Ihr Unternehmen, um umfangreiche Migrationen zu beschleunigen.

ML

Siehe maschinelles Lernen.

Modernisierung

Umwandlung einer veralteten (veralteten oder monolithischen) Anwendung und ihrer Infrastruktur in ein agiles, elastisches und hochverfügbares System in der Cloud, um Kosten zu senken, die Effizienz zu steigern und Innovationen zu nutzen. Weitere Informationen finden Sie unter Strategie zur Modernisierung von Anwendungen in der AWS Cloud.

Bewertung der Modernisierungsfähigkeit

Eine Bewertung, anhand derer festgestellt werden kann, ob die Anwendungen einer Organisation für die Modernisierung bereit sind, Vorteile, Risiken und Abhängigkeiten identifiziert und ermittelt

wird, wie gut die Organisation den zukünftigen Status dieser Anwendungen unterstützen kann. Das Ergebnis der Bewertung ist eine Vorlage der Zielarchitektur, eine Roadmap, in der die Entwicklungsphasen und Meilensteine des Modernisierungsprozesses detailliert beschrieben werden, sowie ein Aktionsplan zur Behebung festgestellter Lücken. Weitere Informationen finden Sie unter Evaluierung der Modernisierungsbereitschaft von Anwendungen in der AWS Cloud.

Monolithische Anwendungen (Monolithen)

Anwendungen, die als ein einziger Service mit eng gekoppelten Prozessen ausgeführt werden. Monolithische Anwendungen haben verschiedene Nachteile. Wenn ein Anwendungs-Feature stark nachgefragt wird, muss die gesamte Architektur skaliert werden. Das Hinzufügen oder Verbessern der Feature einer monolithischen Anwendung wird ebenfalls komplexer, wenn die Codebasis wächst. Um diese Probleme zu beheben, können Sie eine Microservices-Architektur verwenden. Weitere Informationen finden Sie unter Zerlegen von Monolithen in Microservices.

MPA

Siehe Bewertung des Migrationsportfolios.

MQTT

Siehe Message Queuing-Telemetrietransport.

Mehrklassen-Klassifizierung

Ein Prozess, der dabei hilft, Vorhersagen für mehrere Klassen zu generieren (wobei eines von mehr als zwei Ergebnissen vorhergesagt wird). Ein ML-Modell könnte beispielsweise fragen: „Ist dieses Produkt ein Buch, ein Auto oder ein Telefon?“ oder „Welche Kategorie von Produkten ist für diesen Kunden am interessantesten?“

veränderbare Infrastruktur

Ein Modell, das die bestehende Infrastruktur für Produktionsworkloads aktualisiert und modifiziert. Um die Konsistenz, Zuverlässigkeit und Vorhersagbarkeit zu verbessern, empfiehlt das AWS Well-Architected Framework die Verwendung einer unveränderlichen Infrastruktur als bewährte Methode.

O

OAC

Siehe Origin Access Control.

EICHE

Siehe Zugriffsidentität von Origin.

COM

Siehe organisatorisches Change-Management.

Offline-Migration

Eine Migrationsmethode, bei der der Quell-Workload während des Migrationsprozesses heruntergefahren wird. Diese Methode ist mit längeren Ausfallzeiten verbunden und wird in der Regel für kleine, unkritische Workloads verwendet.

OI

Siehe Betriebsintegration.

OLA

Siehe Vereinbarung auf operativer Ebene.

Online-Migration

Eine Migrationsmethode, bei der der Quell-Workload auf das Zielsystem kopiert wird, ohne offline genommen zu werden. Anwendungen, die mit dem Workload verbunden sind, können während der Migration weiterhin funktionieren. Diese Methode beinhaltet keine bis minimale Ausfallzeit und wird in der Regel für kritische Produktionsworkloads verwendet.

OPC-UA

Siehe Open Process Communications — Unified Architecture.

Offene Prozesskommunikation — Einheitliche Architektur (OPC-UA)

Ein Machine-to-Machine-Kommunikationsprotokoll (M2M) für die industrielle Automatisierung. OPC-UA bietet einen Interoperabilitätsstandard mit Datenverschlüsselungs-, Authentifizierungs- und Autorisierungsschemata.

Vereinbarung auf Betriebsebene (OLA)

Eine Vereinbarung, in der klargestellt wird, welche funktionalen IT-Gruppen sich gegenseitig versprechen zu liefern, um ein Service Level Agreement (SLA) zu unterstützen.

Überprüfung der Betriebsbereitschaft (ORR)

Eine Checkliste mit Fragen und zugehörigen bewährten Methoden, die Ihnen helfen, Vorfälle und mögliche Ausfälle zu verstehen, zu bewerten, zu verhindern oder deren Umfang zu reduzieren.

Weitere Informationen finden Sie unter Operational Readiness Readiness Reviews (ORR) im AWS Well-Architected Framework.

Betriebstechnologie (OT)

Hardware- und Softwaresysteme, die mit der physischen Umgebung zusammenarbeiten, um industrielle Abläufe, Ausrüstung und Infrastruktur zu steuern. In der Fertigung ist die Integration von OT- und Informationstechnologie (IT) -Systemen ein zentraler Schwerpunkt der Industrie 4.0-Transformationen.

Betriebsintegration (OI)

Der Prozess der Modernisierung von Abläufen in der Cloud, der Bereitschaftsplanung, Automatisierung und Integration umfasst. Weitere Informationen finden Sie im Leitfaden zur Betriebsintegration.

Organisationspfad

Ein Pfad, der von erstellt wird und in AWS CloudTrail dem alle Ereignisse für alle AWS-Konten in einer Organisation protokolliert werden. AWS Organizations Diese Spur wird in jedem AWS-Konto , der Teil der Organisation ist, erstellt und verfolgt die Aktivität in jedem Konto. Weitere Informationen finden Sie in der CloudTrail Dokumentation unter Einen Trail für eine Organisation erstellen.

Organisatorisches Veränderungsmanagement (OCM)

Ein Framework für das Management wichtiger, disruptiver Geschäftstransformationen aus Sicht der Mitarbeiter, der Kultur und der Führung. OCM hilft Organisationen dabei, sich auf neue Systeme und Strategien vorzubereiten und auf diese umzustellen, indem es die Akzeptanz von Veränderungen beschleunigt, Übergangsprobleme angeht und kulturelle und organisatorische Veränderungen vorantreibt. In der AWS Migrationsstrategie wird dieses Framework aufgrund der Geschwindigkeit des Wandels, der bei Projekten zur Cloud-Einführung erforderlich ist, als Mitarbeiterbeschleunigung bezeichnet. Weitere Informationen finden Sie im OCM-Handbuch.

Ursprungszugriffskontrolle (OAC)

In CloudFront, eine erweiterte Option zur Zugriffsbeschränkung, um Ihre Amazon Simple Storage Service (Amazon S3) -Inhalte zu sichern. OAC unterstützt alle S3-Buckets insgesamt AWS-Regionen, serverseitige Verschlüsselung mit AWS KMS (SSE-KMS) sowie dynamische PUT und `DELETE` Anfragen an den S3-Bucket.

Ursprungszugriffsidentität (OAI)

In CloudFront, eine Option zur Zugriffsbeschränkung, um Ihre Amazon S3 S3-Inhalte zu sichern. Wenn Sie OAI verwenden, CloudFront erstellt es einen Principal, mit dem sich Amazon S3 authentifizieren kann. Authentifizierte Principals können nur über eine bestimmte Distribution auf Inhalte in einem S3-Bucket zugreifen. CloudFront Siehe auch OAC, das eine detailliertere und verbesserte Zugriffskontrolle bietet.

ORR

Weitere Informationen finden Sie unter Überprüfung der Betriebsbereitschaft.

NICHT

Siehe Betriebstechnologie.

Ausgehende (egress) VPC

In einer Architektur AWS mit mehreren Konten eine VPC, die Netzwerkverbindungen verarbeitet, die von einer Anwendung aus initiiert werden. Die AWS -Referenzarchitektur für die Sicherheit empfiehlt, Ihr Netzwerkkonto mit eingehenden und ausgehenden VPCs und Inspektions-VPCs einzurichten, um die bidirektionale Schnittstelle zwischen Ihrer Anwendung und dem Internet zu schützen.

P

Berechtigungsgrenze

Eine IAM-Verwaltungsrichtlinie, die den IAM-Prinzipalen zugeordnet ist, um die maximalen Berechtigungen festzulegen, die der Benutzer oder die Rolle haben kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitys in der IAM-Dokumentation.

persönlich identifizierbare Informationen (PII)

Informationen, die, wenn sie direkt betrachtet oder mit anderen verwandten Daten kombiniert werden, verwendet werden können, um vernünftige Rückschlüsse auf die Identität einer Person zu ziehen. Beispiele für personenbezogene Daten sind Namen, Adressen und Kontaktinformationen.

Personenbezogene Daten

Siehe persönlich identifizierbare Informationen.

Playbook

Eine Reihe vordefinierter Schritte, die die mit Migrationen verbundenen Aufgaben erfassen, z. B. die Bereitstellung zentraler Betriebsfunktionen in der Cloud. Ein Playbook kann die Form von Skripten, automatisierten Runbooks oder einer Zusammenfassung der Prozesse oder Schritte annehmen, die für den Betrieb Ihrer modernisierten Umgebung erforderlich sind.

PLC

Siehe programmierbare Logiksteuerung.

PLM

Siehe Produktlebenszyklusmanagement.

policy

Ein Objekt, das Berechtigungen definieren (siehe identitätsbasierte Richtlinie), Zugriffsbedingungen spezifizieren (siehe ressourcenbasierte Richtlinie) oder die maximalen Berechtigungen für alle Konten in einer Organisation definieren kann AWS Organizations (siehe Dienststeuerungsrichtlinie).

Polyglotte Beharrlichkeit

Unabhängige Auswahl der Datenspeichertechnologie eines Microservices auf der Grundlage von Datenzugriffsmustern und anderen Anforderungen. Wenn Ihre Microservices über dieselbe Datenspeichertechnologie verfügen, kann dies zu Implementierungsproblemen oder zu Leistungseinbußen führen. Microservices lassen sich leichter implementieren und erzielen eine bessere Leistung und Skalierbarkeit, wenn sie den Datenspeicher verwenden, der ihren Anforderungen am besten entspricht.

Portfoliobewertung

Ein Prozess, bei dem das Anwendungsportfolio ermittelt, analysiert und priorisiert wird, um die Migration zu planen. Weitere Informationen finden Sie in Bewerten der Migrationsbereitschaft.

predicate

Eine Abfragebedingung, die `true` oder zurückgibt`false`, was üblicherweise in einer Klausel vorkommt. `WHERE`

Prädikat Pushdown

Eine Technik zur Optimierung von Datenbankabfragen, bei der die Daten in der Abfrage vor der Übertragung gefiltert werden. Dadurch wird die Datenmenge reduziert, die aus der relationalen Datenbank abgerufen und verarbeitet werden muss, und die Abfrageleistung wird verbessert.

Präventive Kontrolle

Eine Sicherheitskontrolle, die verhindern soll, dass ein Ereignis eintritt. Diese Kontrollen stellen eine erste Verteidigungslinie dar, um unbefugten Zugriff oder unerwünschte Änderungen an Ihrem Netzwerk zu verhindern. Weitere Informationen finden Sie unter Präventive Kontrolle in Implementierung von Sicherheitskontrollen in AWS.

Prinzipal

Eine Entität AWS , die Aktionen ausführen und auf Ressourcen zugreifen kann. Bei dieser Entität handelt es sich in der Regel um einen Root-Benutzer für eine AWS-Konto, eine IAM-Rolle oder einen Benutzer. Weitere Informationen finden Sie unter Prinzipal in Rollenbegriffe und -konzepte in der IAM-Dokumentation.

Datenschutz von Natur aus

Ein systemtechnischer Ansatz, der den Datenschutz während des gesamten Entwicklungsprozesses berücksichtigt.

Privat gehostete Zonen

Ein Container, der Informationen darüber enthält, wie Amazon Route 53 auf DNS-Abfragen für eine Domain und ihre Subdomains innerhalb einer oder mehrerer VPCs reagieren soll. Weitere Informationen finden Sie unter Arbeiten mit privat gehosteten Zonen in der Route-53-Dokumentation.

proaktive Steuerung

Eine Sicherheitskontrolle, die den Einsatz nicht richtlinienkonformer Ressourcen verhindern soll. Mit diesen Steuerelementen werden Ressourcen gescannt, bevor sie bereitgestellt werden. Wenn die Ressource nicht mit der Steuerung konform ist, wird sie nicht bereitgestellt. Weitere Informationen finden Sie im Referenzhandbuch zu Kontrollen in der AWS Control Tower Dokumentation und unter Proaktive Kontrollen unter Implementierung von Sicherheitskontrollen am AWS.

Produktlebenszyklusmanagement (PLM)

Das Management von Daten und Prozessen für ein Produkt während seines gesamten Lebenszyklus, vom Design, der Entwicklung und Markteinführung über Wachstum und Reife bis hin zur Markteinführung und Markteinführung.

Produktionsumgebung

Siehe Umgebung.

Speicherprogrammierbare Steuerung (SPS)

In der Fertigung ein äußerst zuverlässiger, anpassungsfähiger Computer, der Maschinen überwacht und Fertigungsprozesse automatisiert.

schnelle Verkettung

Verwenden Sie die Ausgabe einer LLM-Eingabeaufforderung als Eingabe für die nächste Aufforderung, um bessere Antworten zu generieren. Diese Technik wird verwendet, um eine komplexe Aufgabe in Unteraufgaben zu unterteilen oder um eine vorläufige Antwort iterativ zu verfeinern oder zu erweitern. Sie trägt dazu bei, die Genauigkeit und Relevanz der Antworten eines Modells zu verbessern und ermöglicht detailliertere, personalisierte Ergebnisse.

Pseudonymisierung

Der Prozess, bei dem persönliche Identifikatoren in einem Datensatz durch Platzhalterwerte ersetzt werden. Pseudonymisierung kann zum Schutz der Privatsphäre beitragen. Pseudonymisierte Daten gelten weiterhin als personenbezogene Daten.

publish/subscribe (pub/sub)

Ein Muster, das asynchrone Kommunikation zwischen Microservices ermöglicht, um die Skalierbarkeit und Reaktionsfähigkeit zu verbessern. In einem auf Microservices basierenden MES kann ein Microservice beispielsweise Ereignismeldungen in einem Kanal veröffentlichen, den andere Microservices abonnieren können. Das System kann neue Microservices hinzufügen, ohne den Veröffentlichungsservice zu ändern.

Q

Abfrageplan

Eine Reihe von Schritten, wie Anweisungen, die für den Zugriff auf die Daten in einem relationalen SQL-Datenbanksystem verwendet werden.

Abfrageplanregression

Wenn ein Datenbankserviceoptimierer einen weniger optimalen Plan wählt als vor einer bestimmten Änderung der Datenbankumgebung. Dies kann durch Änderungen an Statistiken, Beschränkungen, Umgebungseinstellungen, Abfrageparameter-Bindungen und Aktualisierungen der Datenbank-Engine verursacht werden.

R

RACI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RAG

Siehe Erweiterte Generierung beim Abrufen.

Ransomware

Eine bösartige Software, die entwickelt wurde, um den Zugriff auf ein Computersystem oder Daten zu blockieren, bis eine Zahlung erfolgt ist.

RASCI-Matrix

Siehe verantwortlich, rechenschaftspflichtig, konsultiert, informiert (RACI).

RCAC

Siehe Zugriffskontrolle für Zeilen und Spalten.

Read Replica

Eine Kopie einer Datenbank, die nur für Lesezwecke verwendet wird. Sie können Abfragen an das Lesereplikat weiterleiten, um die Belastung auf Ihrer Primärdatenbank zu reduzieren.

neu strukturieren

Siehe 7 Rs.

Recovery Point Objective (RPO)

Die maximal zulässige Zeitspanne seit dem letzten Datenwiederherstellungspunkt. Damit wird festgelegt, was als akzeptabler Datenverlust zwischen dem letzten Wiederherstellungspunkt und der Serviceunterbrechung gilt.

Wiederherstellungszeitziel (RTO)

Die maximal zulässige Verzögerung zwischen der Betriebsunterbrechung und der Wiederherstellung des Dienstes.

Refaktorierung

Siehe 7 Rs.

Region

Eine Sammlung von AWS Ressourcen in einem geografischen Gebiet. Jeder AWS-Region ist isoliert und unabhängig von den anderen, um Fehlertoleranz, Stabilität und Belastbarkeit zu gewährleisten. Weitere Informationen finden Sie unter Geben Sie an, was AWS-Regionen Ihr Konto verwenden kann.

Regression

Eine ML-Technik, die einen numerischen Wert vorhersagt. Zum Beispiel, um das Problem „Zu welchem Preis wird dieses Haus verkauft werden?“ zu lösen Ein ML-Modell könnte ein lineares Regressionsmodell verwenden, um den Verkaufspreis eines Hauses auf der Grundlage bekannter Fakten über das Haus (z. B. die Quadratmeterzahl) vorherzusagen.

rehosten

Siehe 7 Rs.

Veröffentlichung

In einem Bereitstellungsprozess der Akt der Förderung von Änderungen an einer Produktionsumgebung.

umziehen

Siehe 7 Rs.

neue Plattform

Siehe 7 Rs.

Rückkauf

Siehe 7 Rs.

Ausfallsicherheit

Die Fähigkeit einer Anwendung, Störungen zu widerstehen oder sich von ihnen zu erholen. Hochverfügbarkeit und Notfallwiederherstellung sind häufig Überlegungen bei der Planung der Ausfallsicherheit in der. AWS Cloud Weitere Informationen finden Sie unter AWS Cloud Resilienz.

Ressourcenbasierte Richtlinie

Eine mit einer Ressource verknüpfte Richtlinie, z. B. ein Amazon-S3-Bucket, ein Endpunkt oder ein Verschlüsselungsschlüssel. Diese Art von Richtlinie legt fest, welchen Prinzipalen der Zugriff gewährt wird, welche Aktionen unterstützt werden und welche anderen Bedingungen erfüllt sein müssen.

RACI-Matrix (verantwortlich, rechenschaftspflichtig, konsultiert, informiert)

Eine Matrix, die die Rollen und Verantwortlichkeiten für alle Parteien definiert, die an Migrationsaktivitäten und Cloud-Vorgängen beteiligt sind. Der Matrixname leitet sich von den in der Matrix definierten Zuständigkeitstypen ab: verantwortlich (R), rechenschaftspflichtig (A), konsultiert (C) und informiert (I). Der Unterstützungstyp (S) ist optional. Wenn Sie Unterstützung einbeziehen, wird die Matrix als RASCI-Matrix bezeichnet, und wenn Sie sie ausschließen, wird sie als RACI-Matrix bezeichnet.

Reaktive Kontrolle

Eine Sicherheitskontrolle, die darauf ausgelegt ist, die Behebung unerwünschter Ereignisse oder Abweichungen von Ihren Sicherheitsstandards voranzutreiben. Weitere Informationen finden Sie unter Reaktive Kontrolle in Implementieren von Sicherheitskontrollen in AWS.

Beibehaltung

Siehe 7 Rs.

zurückziehen

Siehe 7 Rs.

Retrieval Augmented Generation (RAG)

Eine generative KI-Technologie, bei der ein LLM auf eine maßgebliche Datenquelle verweist, die sich außerhalb seiner Trainingsdatenquellen befindet, bevor eine Antwort generiert wird. Ein RAG-Modell könnte beispielsweise eine semantische Suche in der Wissensdatenbank oder in benutzerdefinierten Daten einer Organisation durchführen. Weitere Informationen finden Sie unter Was ist RAG.

Drehung

Der Vorgang, bei dem ein Geheimnis regelmäßig aktualisiert wird, um es einem Angreifer zu erschweren, auf die Anmeldeinformationen zuzugreifen.

Zugriffskontrolle für Zeilen und Spalten (RCAC)

Die Verwendung einfacher, flexibler SQL-Ausdrücke mit definierten Zugriffsregeln. RCAC besteht aus Zeilenberechtigungen und Spaltenmasken.

RPO

Siehe Recovery Point Objective.

RTO

Siehe Ziel für die Erholungszeit.

Runbook

Eine Reihe manueller oder automatisierter Verfahren, die zur Ausführung einer bestimmten Aufgabe erforderlich sind. Diese sind in der Regel darauf ausgelegt, sich wiederholende Operationen oder Verfahren mit hohen Fehlerquoten zu rationalisieren.

S

SAML 2.0

Ein offener Standard, den viele Identitätsanbieter (IdPs) verwenden. Diese Funktion ermöglicht föderiertes Single Sign-On (SSO), sodass sich Benutzer bei den API-Vorgängen anmelden AWS-Managementkonsole oder die AWS API-Operationen aufrufen können, ohne dass Sie einen Benutzer in IAM für alle in Ihrer Organisation erstellen müssen. Weitere Informationen zum SAML-2.0.-basierten Verbund finden Sie unter Über den SAML-2.0-basierten Verbund in der IAM-Dokumentation.

SCADA

Siehe Aufsichtskontrolle und Datenerfassung.

SCP

Siehe Richtlinie zur Dienstkontrolle.

Secret

Interne AWS Secrets Manager, vertrauliche oder eingeschränkte Informationen, wie z. B. ein Passwort oder Benutzeranmeldedaten, die Sie in verschlüsselter Form speichern. Es besteht aus dem geheimen Wert und seinen Metadaten. Der geheime Wert kann binär, eine einzelne Zeichenfolge oder mehrere Zeichenketten sein. Weitere Informationen finden Sie unter Was ist in einem Secrets Manager Manager-Geheimnis? in der Secrets Manager Manager-Dokumentation.

Sicherheit durch Design

Ein systemtechnischer Ansatz, der die Sicherheit während des gesamten Entwicklungsprozesses berücksichtigt.

Sicherheitskontrolle

Ein technischer oder administrativer Integritätsschutz, der die Fähigkeit eines Bedrohungsakteurs, eine Schwachstelle auszunutzen, verhindert, erkennt oder einschränkt. Es gibt vier Haupttypen von Sicherheitskontrollen: präventiv, detektiv, reaktionsschnell und proaktiv.

Härtung der Sicherheit

Der Prozess, bei dem die Angriffsfläche reduziert wird, um sie widerstandsfähiger gegen Angriffe zu machen. Dies kann Aktionen wie das Entfernen von Ressourcen, die nicht mehr benötigt werden, die Implementierung der bewährten Sicherheitsmethode der Gewährung geringster Berechtigungen oder die Deaktivierung unnötiger Feature in Konfigurationsdateien umfassen.

System zur Verwaltung von Sicherheitsinformationen und Ereignissen (security information and event management – SIEM)

Tools und Services, die Systeme für das Sicherheitsinformationsmanagement (SIM) und das Management von Sicherheitsereignissen (SEM) kombinieren. Ein SIEM-System sammelt, überwacht und analysiert Daten von Servern, Netzwerken, Geräten und anderen Quellen, um Bedrohungen und Sicherheitsverletzungen zu erkennen und Warnmeldungen zu generieren.

Automatisierung von Sicherheitsreaktionen

Eine vordefinierte und programmierte Aktion, die darauf ausgelegt ist, automatisch auf ein Sicherheitsereignis zu reagieren oder es zu beheben. Diese Automatisierungen dienen als detektive oder reaktionsschnelle Sicherheitskontrollen, die Sie bei der Implementierung bewährter AWS Sicherheitsmethoden unterstützen. Beispiele für automatisierte Antwortaktionen sind das Ändern einer VPC-Sicherheitsgruppe, das Patchen einer Amazon EC2 EC2-Instance oder das Rotieren von Anmeldeinformationen.

Serverseitige Verschlüsselung

Verschlüsselung von Daten am Zielort durch denjenigen AWS-Service , der sie empfängt.

Service-Kontrollrichtlinie (SCP)

Eine Richtlinie, die eine zentrale Kontrolle über die Berechtigungen für alle Konten in einer Organisation in AWS Organizations ermöglicht. SCPs definieren Integritätsschutz oder legen Grenzwerte für Aktionen fest, die ein Administrator an Benutzer oder Rollen delegieren kann. Sie können SCPs als Zulassungs- oder Ablehnungslisten verwenden, um festzulegen, welche Services oder Aktionen zulässig oder verboten sind. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Richtlinien zur Dienststeuerung.

Service-Endpunkt

Die URL des Einstiegspunkts für einen AWS-Service. Sie können den Endpunkt verwenden, um programmgesteuert eine Verbindung zum Zielservice herzustellen. Weitere Informationen finden Sie unter AWS-Service -Endpunkte in der Allgemeine AWS-Referenz.

Service Level Agreement (SLA)

Eine Vereinbarung, in der klargestellt wird, was ein IT-Team seinen Kunden zu bieten verspricht, z. B. in Bezug auf Verfügbarkeit und Leistung der Services.

Service-Level-Indikator (SLI)

Eine Messung eines Leistungsaspekts eines Dienstes, z. B. seiner Fehlerrate, Verfügbarkeit oder Durchsatz.

Service-Level-Ziel (SLO)

Eine Zielkennzahl, die den Zustand eines Dienstes darstellt, gemessen anhand eines Service-Level-Indikators.

Modell der geteilten Verantwortung

Ein Modell, das die Verantwortung beschreibt, mit der Sie gemeinsam AWS für Cloud-Sicherheit und Compliance verantwortlich sind. AWS ist für die Sicherheit der Cloud verantwortlich, während Sie für die Sicherheit in der Cloud verantwortlich sind. Weitere Informationen finden Sie unter Modell der geteilten Verantwortung.

Schatten-KI

Nicht autorisierte KI-Anwendungen, die außerhalb der kontrollierten Kanäle innerhalb eines Unternehmens erstellt oder verwendet wurden.

SIEM

Siehe Sicherheitsinformations- und Event-Management-System.

Single Point of Failure (SPOF)

Ein Fehler in einer einzelnen, kritischen Komponente einer Anwendung, der das System stören kann.

SLA

Siehe Service Level Agreement.

SLI

Siehe Service-Level-Indikator.

ALSO

Siehe Service-Level-Ziel.

Split-and-Seed-Modell

Ein Muster für die Skalierung und Beschleunigung von Modernisierungsprojekten. Sobald neue Features und Produktversionen definiert werden, teilt sich das Kernteam auf, um neue Produktteams zu bilden. Dies trägt zur Skalierung der Fähigkeiten und Services Ihrer Organisation bei, verbessert die Produktivität der Entwickler und unterstützt schnelle Innovationen. Weitere Informationen finden Sie unter Schrittweiser Ansatz zur Modernisierung von Anwendungen in der. AWS Cloud

SPOTTEN

Siehe Single Point of Failure.

Sternschema

Eine Datenbank-Organisationsstruktur, die eine große Faktentabelle zum Speichern von Transaktions- oder Messdaten und eine oder mehrere kleinere dimensionale Tabellen zum Speichern von Datenattributen verwendet. Diese Struktur ist für die Verwendung in einem Data Warehouse oder für Business Intelligence-Zwecke konzipiert.

Strangler-Fig-Muster

Ein Ansatz zur Modernisierung monolithischer Systeme, bei dem die Systemfunktionen schrittweise umgeschrieben und ersetzt werden, bis das Legacy-System außer Betrieb genommen werden kann. Dieses Muster verwendet die Analogie einer Feigenrebe, die zu einem etablierten Baum heranwächst und schließlich ihren Wirt überwindet und ersetzt. Das Muster wurde eingeführt von Martin Fowler als Möglichkeit, Risiken beim Umschreiben monolithischer Systeme zu managen. Ein Beispiel für die Anwendung dieses Musters finden Sie unter Schrittweise Modernisierung älterer Microsoft ASP.NET (ASMX) -Webservices mithilfe von Containern und Amazon API Gateway.

Subnetz

Ein Bereich von IP-Adressen in Ihrer VPC. Ein Subnetz muss sich in einer einzigen Availability Zone befinden.

Aufsichtskontrolle und Datenerfassung (SCADA)

In der Fertigung ein System, das Hardware und Software zur Überwachung von Sachanlagen und Produktionsabläufen verwendet.

Symmetrische Verschlüsselung

Ein Verschlüsselungsalgorithmus, der denselben Schlüssel zum Verschlüsseln und Entschlüsseln der Daten verwendet.

synthetisches Testen

Testen eines Systems auf eine Weise, die Benutzerinteraktionen simuliert, um potenzielle Probleme zu erkennen oder die Leistung zu überwachen. Sie können Amazon CloudWatch Synthetics verwenden, um diese Tests zu erstellen.

Systemaufforderung

Eine Technik, mit der einem LLM Kontext, Anweisungen oder Richtlinien zur Verfügung gestellt werden, um sein Verhalten zu steuern. Systemaufforderungen helfen dabei, den Kontext festzulegen und Regeln für Interaktionen mit Benutzern festzulegen.

T

tags

Key-value Paare, die als Metadaten für die Organisation Ihrer AWS Ressourcen dienen. Mit Tags können Sie Ressourcen verwalten, identifizieren, organisieren, suchen und filtern. Weitere Informationen finden Sie unter Markieren Ihrer AWS -Ressourcen.

Zielvariable

Der Wert, den Sie in überwachtem ML vorhersagen möchten. Dies wird auch als Ergebnisvariable bezeichnet. In einer Fertigungsumgebung könnte die Zielvariable beispielsweise ein Produktfehler sein.

Aufgabenliste

Ein Tool, das verwendet wird, um den Fortschritt anhand eines Runbooks zu verfolgen. Eine Aufgabenliste enthält eine Übersicht über das Runbook und eine Liste mit allgemeinen Aufgaben, die erledigt werden müssen. Für jede allgemeine Aufgabe werden der geschätzte Zeitaufwand, der Eigentümer und der Fortschritt angegeben.

Testumgebungen

Siehe Umgebung.

Training

Daten für Ihr ML-Modell bereitstellen, aus denen es lernen kann. Die Trainingsdaten müssen die richtige Antwort enthalten. Der Lernalgorithmus findet Muster in den Trainingsdaten, die die Attribute der Input-Daten dem Ziel (die Antwort, die Sie voraussagen möchten) zuordnen. Es gibt ein ML-Modell aus, das diese Muster erfasst. Sie können dann das ML-Modell verwenden, um Voraussagen für neue Daten zu erhalten, bei denen Sie das Ziel nicht kennen.

tool

Eine Funktion oder API, die ein Agent aufrufen kann, um Operationen in externen Systemen auszuführen.

Transit-Gateway

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und On-Premises-Netzwerke miteinander verbinden können. Weitere Informationen finden Sie in der AWS Transit Gateway Dokumentation unter Was ist ein Transit-Gateway.

Stammbasierter Workflow

Ein Ansatz, bei dem Entwickler Feature lokal in einem Feature-Zweig erstellen und testen und diese Änderungen dann im Hauptzweig zusammenführen. Der Hauptzweig wird dann sequentiell für die Entwicklungs-, Vorproduktions- und Produktionsumgebungen erstellt.

Vertrauenswürdiger Zugriff

Gewährung von Berechtigungen für einen Dienst, den Sie angeben, um Aufgaben in Ihrer Organisation AWS Organizations und in deren Konten in Ihrem Namen auszuführen. Der vertrauenswürdige Service erstellt in jedem Konto eine mit dem Service verknüpfte Rolle, wenn diese Rolle benötigt wird, um Verwaltungsaufgaben für Sie auszuführen. Weitere Informationen finden Sie in der AWS Organizations Dokumentation unter Verwendung AWS Organizations mit anderen AWS Diensten.

Optimieren

Aspekte Ihres Trainingsprozesses ändern, um die Genauigkeit des ML-Modells zu verbessern. Sie können das ML-Modell z. B. trainieren, indem Sie einen Beschriftungssatz generieren, Beschriftungen hinzufügen und diese Schritte dann mehrmals unter verschiedenen Einstellungen wiederholen, um das Modell zu optimieren.

Zwei-Pizzen-Team

Ein kleines DevOps Team, das Sie mit zwei Pizzen ernähren können. Eine Teamgröße von zwei Pizzen gewährleistet die bestmögliche Gelegenheit zur Zusammenarbeit bei der Softwareentwicklung.

U

Unsicherheit

Ein Konzept, das sich auf ungenaue, unvollständige oder unbekannte Informationen bezieht, die die Zuverlässigkeit von prädiktiven ML-Modellen untergraben können. Es gibt zwei Arten von Unsicherheit: Epistemische Unsicherheit wird durch begrenzte, unvollständige Daten verursacht, wohingegen aleatorische Unsicherheit durch Rauschen und Randomisierung verursacht wird, die in den Daten liegt.

undifferenzierte Aufgaben

Diese Arbeit wird auch als Schwerstarbeit bezeichnet. Dabei handelt es sich um Arbeiten, die zwar für die Erstellung und den Betrieb einer Anwendung erforderlich sind, aber dem Endbenutzer keinen direkten Mehrwert bieten oder keinen Wettbewerbsvorteil bieten. Beispiele für undifferenzierte Aufgaben sind Beschaffung, Wartung und Kapazitätsplanung.

höhere Umgebungen

Siehe Umgebung.

V

Vacuuming

Ein Vorgang zur Datenbankwartung, bei dem die Datenbank nach inkrementellen Aktualisierungen bereinigt wird, um Speicherplatz zurückzugewinnen und die Leistung zu verbessern.

Versionskontrolle

Prozesse und Tools zur Nachverfolgung von Änderungen, z. B. Änderungen am Quellcode in einem Repository.

VPC-Peering

Eine Verbindung zwischen zwei VPCs, mit der Sie den Datenverkehr mithilfe von privaten IP-Adressen weiterleiten können. Weitere Informationen finden Sie unter Was ist VPC-Peering? in der Amazon-VPC-Dokumentation.

Schwachstelle

Ein Software- oder Hardwarefehler, der die Sicherheit des Systems gefährdet.

W

Warmer Cache

Ein Puffer-Cache, der aktuelle, relevante Daten enthält, auf die häufig zugegriffen wird. Die Datenbank-Instance kann aus dem Puffer-Cache lesen, was schneller ist als das Lesen aus dem Hauptspeicher oder von der Festplatte.

warme Daten

Daten, auf die selten zugegriffen wird. Bei der Abfrage dieser Art von Daten sind mäßig langsame Abfragen in der Regel akzeptabel.

Fensterfunktion

Eine SQL-Funktion, die eine Berechnung für eine Gruppe von Zeilen durchführt, die sich in irgendeiner Weise auf den aktuellen Datensatz beziehen. Fensterfunktionen sind nützlich für die Verarbeitung von Aufgaben wie die Berechnung eines gleitenden Durchschnitts oder für den Zugriff auf den Wert von Zeilen auf der Grundlage der relativen Position der aktuellen Zeile.

Workload

Ein Workload ist eine Sammlung von Ressourcen und Code, die einen Unternehmenswert bietet, wie z. B. eine kundenorientierte Anwendung oder ein Backend-Prozess.

Workstream

Funktionsgruppen in einem Migrationsprojekt, die für eine bestimmte Reihe von Aufgaben verantwortlich sind. Jeder Workstream ist unabhängig, unterstützt aber die anderen Workstreams im Projekt. Der Portfolio-Workstream ist beispielsweise für die Priorisierung von Anwendungen, die Wellenplanung und die Erfassung von Migrationsmetadaten verantwortlich. Der Portfolio-Workstream liefert diese Komponenten an den Migrations-Workstream, der dann die Server und Anwendungen migriert.

WURM

Mal schreiben, viele lesen.

WQF

Siehe AWS Workload-Qualifizierungsrahmen.

einmal schreiben, viele lesen (WORM)

Ein Speichermodell, das Daten ein einziges Mal schreibt und verhindert, dass die Daten gelöscht oder geändert werden. Autorisierte Benutzer können die Daten so oft wie nötig lesen, aber sie können sie nicht ändern. Diese Datenspeicherinfrastruktur wird als unveränderlich angesehen.

Z

Zero-Day-Exploit

Ein Angriff, in der Regel Malware, der eine Zero-Day-Sicherheitslücke ausnutzt.

Zero-Day-Sicherheitslücke

Ein unfehlbarer Fehler oder eine Sicherheitslücke in einem Produktionssystem. Bedrohungsakteure können diese Art von Sicherheitslücke nutzen, um das System anzugreifen. Entwickler werden aufgrund des Angriffs häufig auf die Sicherheitsanfälligkeit aufmerksam.

Eingabeaufforderung ohne Vorwarnung

Bereitstellung von Anweisungen für die Ausführung einer Aufgabe an einen LLM, jedoch ohne Beispiele (Schnappschüsse), die ihm als Orientierungshilfe dienen könnten. Der LLM muss sein vortrainiertes Wissen einsetzen, um die Aufgabe zu bewältigen. Die Effektivität von Zero-Shot Prompting hängt von der Komplexität der Aufgabe und der Qualität der Aufforderung ab. Siehe auch Few-Shot-Eingabeaufforderungen.

Zombie-Anwendung

Eine Anwendung, deren durchschnittliche CPU- und Arbeitsspeichernutzung unter 5 Prozent liegt. In einem Migrationsprojekt ist es üblich, diese Anwendungen außer Betrieb zu nehmen.

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.