Implementazione di una strategia di controllo dei bot su AWS

AWS Guida prescrittiva

AWS Guida prescrittiva: Implementazione di una strategia di controllo dei bot su AWS

Table of Contents

Implementazione di una strategia di controllo dei bot su AWS

Amazon Web Services (collaboratori)

Febbraio 2024 (cronologia dei documenti)

Internet così come lo conosciamo non sarebbe possibile senza i bot. I bot eseguono attività automatizzate su Internet e simulano l'attività o l'interazione umana. Consentono alle aziende di aumentare l'efficienza dei processi e delle attività. Bot utili, come i web crawler, indicizzano le informazioni su Internet e ci aiutano a trovare rapidamente le informazioni più pertinenti per le nostre query di ricerca. I bot sono un buon meccanismo per migliorare il business e fornire valore alle aziende. Tuttavia, con il tempo, i malintenzionati hanno iniziato a utilizzare i bot come mezzo per abusare dei sistemi e delle applicazioni esistenti in modi nuovi e creativi.

Le botnet sono il meccanismo più noto per scalare i bot e il loro impatto. Le botnet sono reti di bot infettate da malware e controllate da un'unica parte, nota come bot herder o bot operator. Da un punto centrale, l'operatore può comandare a tutti i computer della sua botnet di eseguire simultaneamente un'azione coordinata, motivo per cui le botnet vengono anche chiamate sistemi (C2). command-and-control

La dimensione di una botnet può essere di diversi milioni di bot. Una botnet aiuta l'operatore a eseguire azioni su larga scala. Poiché le botnet rimangono sotto il controllo di un operatore remoto, le macchine infette possono ricevere aggiornamenti e modificare il proprio comportamento all'istante. Di conseguenza, con un notevole guadagno finanziario, i sistemi C2 possono affittare l'accesso a segmenti della loro botnet sul mercato nero.

La prevalenza delle botnet ha continuato a crescere. È considerato dagli esperti lo strumento preferito dai cattivi attori. Mirai è una delle botnet più grandi. È emerso nel 2016, è ancora operativo e si stima che abbia infettato fino a 350.000 dispositivi Internet of Things (IoT). Questa botnet è stata adattata e utilizzata per molti tipi di attività, inclusi gli attacchi DDoS (Distributed Denial of Service). Più recentemente, i malintenzionati hanno cercato di offuscare ulteriormente la loro attività e di ottenere traffico ottenendo indirizzi IP tramite l'uso di servizi proxy residenziali. Ciò crea un peer-to-peer sistema legittimo e interconnesso che aggiunge sofisticazione all'attività e la rende più difficile da rilevare e mitigare.

Questo documento si concentra sul panorama dei bot, sul loro effetto sulle applicazioni e sulle strategie e opzioni di mitigazione disponibili. Questa guida prescrittiva e le relative best practice aiutano a comprendere e mitigare diversi tipi di attacchi bot. Inoltre, questa guida descrive le Servizi

AWS funzionalità che supportano una strategia di mitigazione dei bot e come ognuna di esse può aiutarti a proteggere le tue applicazioni. Include anche una panoramica del monitoraggio dei bot e delle migliori pratiche per ottimizzare i costi delle soluzioni.

Comprendere le minacce e le operazioni dei bot

Secondo Security Today, oltre il 47% di tutto il traffico su Internet è dovuto ai bot. Ciò include la parte utile dei bot, quelli che si autoidentificano e forniscono valore. Circa il 30% del traffico bot è costituito da bot non identificati che svolgono attività dannose, come attacchi DDoS, ticket scalping, analisi dell'inventario o accumulo di dati. Security Magazine riporta un aumento del 300% degli eventi DDoS volumetrici nella prima metà del 2023. Ciò rende questo argomento più pertinente e rende ancora più importante la conoscenza degli strumenti e delle tecnologie di prevenzione e protezione disponibili.

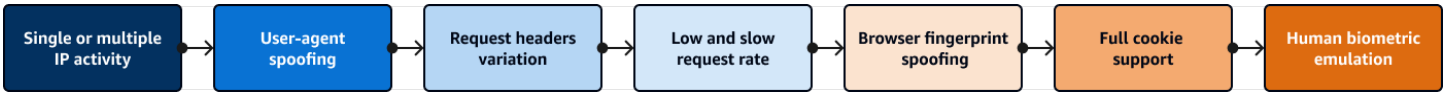
La tabella seguente classifica i diversi tipi di attività dei bot e l'impatto aziendale che ciascuna di esse può avere. Questo non vuole essere un elenco esaustivo; è un riepilogo delle attività dei bot più comuni. Sottolinea l'importanza del monitoraggio e dei controlli di mitigazione. Per un elenco completo delle minacce dei bot, consulta il manuale OWASP Automated Threats to applications (sito web OWASP).

Tipo di attività dei bot	Descrizione	Impatto potenziale
Raschiamento dei contenuti	Copia di contenuti proprietari per l'utilizzo da parte di siti di terze parti	Impatto sulla SEO dovuto alla duplicazione dei contenuti, all'impatto sul marchio e ai problemi di prestazioni causati da scraper aggressivi
Riempimento di credenziali	Verifica dei database di credenziali rubati presenti nel vostro sito web per ottenere l'accesso o convalidare le informazioni	Problemi per gli utenti, come frodi e blocchi degli account, che aumentano le richieste di assistenza e riducono la fiducia del marchio
Incrinatura delle carte	Analisi dei database dei dati delle carte di credito rubate per convalidare o integrare le informazioni mancanti	Problemi per gli utenti, come furto di identità e frode, e danni al punteggio di frode
Negazione del servizio	Aumentare il traffico verso un sito Web specifico per rallentar e la risposta o renderlo non	Perdita di ricavi e danni alla reputazione

Tipo di attività dei bot	Descrizione	Impatto potenziale
	disponibile per il traffico legittimo	
Creazione di un account	Creazione di più account a scopo di uso improprio o di lucro	Crescita ostacolata e analisi di marketing distorte
Scalping	Ottenere beni a disponibi lità limitata, spesso biglietti d'ingresso, rispetto a veri consumatori	Perdita di entrate e problemi per gli utenti, come la mancanza di accesso ai beni venduti

Come funzionano le botnet

Le tattiche, le tecniche e le procedure (TTP) degli operatori di botnet si sono evolute notevolmente nel tempo. Hanno dovuto tenere il passo con le tecnologie di rilevamento e mitigazione sviluppate dalle aziende. La figura seguente mostra questa evoluzione. Le botnet hanno iniziato semplicemente utilizzando gli indirizzi IP come mezzo operativo e alla fine si sono evolute per utilizzare una sofisticata emulazione biometrica umana. Questa sofisticazione è costosa e non tutte le botnet utilizzano gli strumenti più avanzati. Gli operatori di Internet sono diversi e probabilmente valutano lo strumento migliore per garantire un buon ritorno sull'investimento. Uno degli obiettivi della difesa dai bot è rendere costosa l'attività delle botnet in modo che l'obiettivo non sia più praticabile.



In generale, i bot sono classificati come comuni o mirati:

- Bot comuni: questi bot si identificano automaticamente e non tentano di emulare i browser. Molti di questi bot svolgono attività utili, come la scansione dei contenuti, l'ottimizzazione dei motori di ricerca (SEO) o l'aggregazione. È importante identificare e comprendere quali di questi bot comuni arrivano sul tuo sito e l'effetto che hanno sul tuo traffico e sulle tue prestazioni.
- Bot mirati: questi bot cercano di eludere il rilevamento emulando i browser. Utilizzano la tecnologia dei browser, come i browser headless, oppure falsificano le impronte digitali del browser. Hanno la

capacità di eseguire JavaScript e supportare i cookie. Il loro intento non è sempre chiaro e il traffico che generano può assomigliare al normale traffico degli utenti.

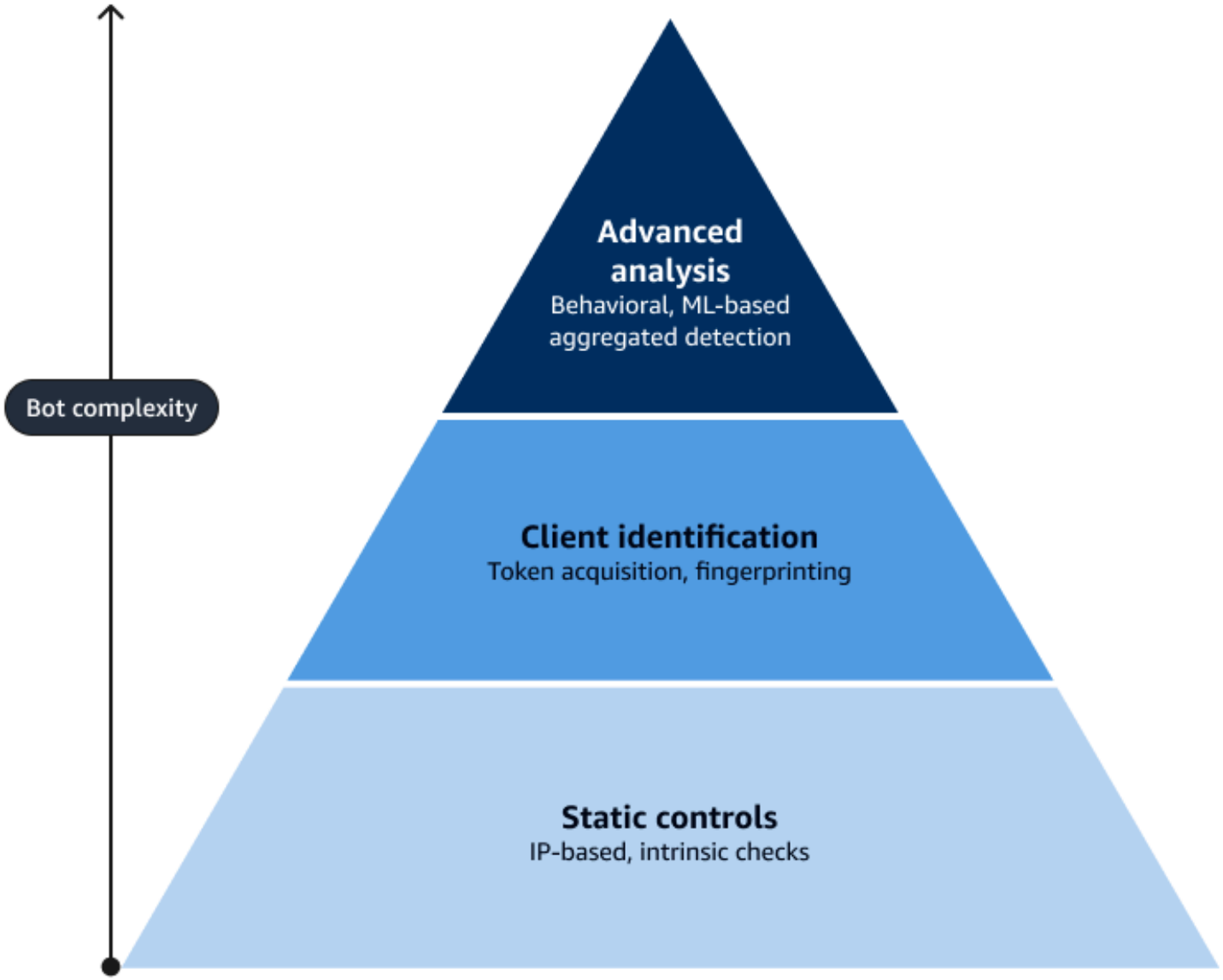
I bot mirati più avanzati e persistenti emulano il comportamento umano generando movimenti e clic del mouse simili a quelli umani su un sito Web. Sono i più sofisticati e difficili da rilevare, ma sono anche i più costosi da utilizzare.

Spesso un operatore combina queste tecniche. Ciò crea un gioco di inseguimento costante, in cui è necessario modificare frequentemente l'approccio di protezione e mitigazione per adattarlo alle tecniche più recenti dell'operatore. Questi bot sono considerati una minaccia persistente avanzata (APT). Per ulteriori informazioni, vedere Minaccia persistente avanzata nel centro risorse del NIST.

Tecniche per il controllo dei bot

L'obiettivo principale della mitigazione dei bot è limitare l'impatto negativo dell'attività automatizzata dei bot sui siti Web, sui servizi e sulle applicazioni di un'organizzazione. La tecnologia e le tecniche utilizzate dipendono dal tipo di traffico o di attività da cui ci si vuole difendere. Comprendere l'applicazione e il relativo traffico è fondamentale per raggiungere questo obiettivo. Per ulteriori informazioni su dove iniziare, consulta la Linee guida per il monitoraggio della strategia di controllo dei bot sezione di questa guida.

In generale, i controlli forniti dalle soluzioni di mitigazione dei bot possono essere raggruppati nelle seguenti categorie di alto livello: statico, identificazione del cliente e analisi avanzata. La figura seguente mostra le diverse tecniche disponibili e come possono essere utilizzate a seconda della complessità dell'attività del bot. Ciò evidenzia come la mitigazione di base, o più ampia, possa essere ottenuta mediante l'uso di controlli statici, come l'elenco degli indirizzi consentiti e i controlli intrinseci. La parte più piccola dei bot è sempre la più avanzata e la mitigazione di questi bot richiede una tecnologia più avanzata e una combinazione di controlli.



Successivamente, questa guida esplora ogni categoria e le relative tecniche. Descrive inoltre le opzioni disponibili AWS WAFper implementare questi controlli:

- Controlli statici per la gestione dei bot
- Controlli di identificazione dei client per la gestione dei bot
- Controlli di analisi avanzati per la gestione dei bot

Controlli statici per la gestione dei bot

Per eseguire un'azione, i controlli statici valutano le informazioni statiche contenute nella richiesta HTTP (S), come l'indirizzo IP o le intestazioni. Questi controlli possono essere utili per attività bot

poco sofisticate o per il traffico di bot vantaggioso previsto che deve essere verificato e gestito. Le tecniche di controllo statico includono: elenco degli indirizzi consentiti, controlli basati su IP e controlli intrinseci.

Consenti la pubblicazione

L'elenco consentito è un controllo che consente l'identificazione di traffico amichevole tramite i controlli di mitigazione dei bot esistenti. Esistono diversi modi per farlo. Il metodo più semplice consiste nell'utilizzare una regola che corrisponda a un insieme di indirizzi IP o a una condizione di corrispondenza simile. Quando una richiesta corrisponde a una regola impostata su un'`Allow`azione, non viene valutata dalle regole successive. In alcuni casi, è necessario impedire che vengano applicate solo determinate regole; in altre parole, è necessario consentire l'elenco di una regola ma non di tutte le regole. Si tratta di uno scenario comune per la gestione dei falsi positivi per le regole. L'opzione Allow listing è considerata una regola di ampio respiro. Per ridurre il rischio di falsi negativi, ti consigliamo di abbinarla a un'altra opzione più granulare, come un percorso o un header match.

Controlli basati su IP

Blocchi di indirizzi IP singoli

Uno strumento comunemente usato per mitigare l'impatto dei bot consiste nel limitare le richieste provenienti da un singolo richiedente. L'esempio più semplice consiste nel bloccare l'indirizzo IP di origine del traffico se le sue richieste sono dannose o hanno un volume elevato. Questo utilizza le regole AWS WAF IP set match per implementare blocchi basati su IP. Queste regole corrispondono agli indirizzi IP e applicano un'azione di `BlockChallenge`, o`CAPTCHA`. È possibile determinare quando arrivano troppe richieste da un indirizzo IP esaminando il Content Delivery Network (CDN), un firewall di applicazioni Web o i registri di applicazioni e servizi. Tuttavia, nella maggior parte dei casi, questo controllo non è pratico senza automazione.

L'automazione degli elenchi di indirizzi IP bloccati AWS WAF viene generalmente eseguita con regole basate sulla frequenza. Per ulteriori informazioni sul tagging, consulta Regole basata sulla frequenzain questa guida. Puoi anche implementare la soluzione Security Automations for. AWS WAF Questa soluzione aggiorna automaticamente un elenco di indirizzi IP da bloccare e una AWS WAF regola nega le richieste che corrispondono a tali indirizzi IP.

Un modo per riconoscere un attacco bot è se una moltitudine di richieste provenienti dallo stesso indirizzo IP si concentra su un numero limitato di pagine Web. Ciò indica che il bot sta abbassando i prezzi o sta tentando ripetutamente di effettuare accessi con esito negativo con una percentuale

elevata. Puoi creare automazioni che riconoscono immediatamente questo schema. Le automazioni bloccano l'indirizzo IP, il che riduce l'efficacia dell'attacco identificandolo e mitigandolo rapidamente. Il blocco di indirizzi IP specifici è meno efficace quando un utente malintenzionato dispone di un'ampia raccolta di indirizzi IP da cui lanciare attacchi o quando il comportamento di attacco è difficile da riconoscere e separare dal traffico normale.

Reputazione degli indirizzi IP

Un servizio di reputazione IP fornisce informazioni che aiutano a valutare l'affidabilità di un indirizzo IP. Questa intelligence viene in genere derivata dall'aggregazione di informazioni relative all'IP relative alle attività passate provenienti da quell'indirizzo IP. Le attività precedenti aiutano a indicare la probabilità che un indirizzo IP generi richieste dannose. I dati vengono aggiunti agli elenchi gestiti che tengono traccia del comportamento degli indirizzi IP.

Gli indirizzi IP anonimi sono un caso specializzato di reputazione degli indirizzi IP. L'indirizzo IP di origine proviene da fonti note di indirizzi IP facilmente acquisibili, come macchine virtuali basate sul cloud, o da proxy, come provider VPN o nodi Tor noti. I gruppi di regole gestiti da AWS WAF Amazon IP Reputation List e Anonymous IP List utilizzano l'intelligence interna di Amazon sulle minacce per identificare questi indirizzi IP.

L'intelligence fornita da questi elenchi gestiti può aiutarti ad agire in base alle attività identificate da queste fonti. Sulla base di queste informazioni, puoi creare regole che bloccano direttamente il traffico o regole che limitano il numero di richieste (come le regole basate sulla tariffa). È inoltre possibile utilizzare questa intelligenza per valutare la fonte del traffico utilizzando le regole in `COUNT` modalità. In questo modo vengono esaminati i criteri di corrispondenza e vengono applicate etichette che è possibile utilizzare per creare regole personalizzate.

Regole basata sulla frequenza

Le regole basate sulle tariffe possono essere uno strumento prezioso per determinati scenari. Ad esempio, le regole basate sulla tariffa sono efficaci quando il traffico dei bot raggiunge volumi elevati rispetto agli utenti che utilizzano identificatori di risorse uniformi (URI) sensibili o quando il volume di traffico inizia a influire sulle normali operazioni. La limitazione della velocità può mantenere le richieste a livelli gestibili e limitare e controllare l'accesso. AWS WAF può implementare una regola di limitazione della velocità in una lista di controllo degli accessi Web (Web ACL) utilizzando una dichiarazione di regola basata sulla velocità. Un approccio consigliato quando si utilizzano regole basate sulla frequenza consiste nell'includere una regola generale che copra l'intero sito, regole specifiche per l'URI e regole basate sulla percentuale di reputazione IP. Le regole basate sulla

percentuale di reputazione IP combinano l'intelligenza della reputazione degli indirizzi IP con la funzionalità di limitazione della velocità.

Per l'intero sito, una regola generale basata sul tasso di reputazione IP crea un limite che impedisce a bot non sofisticati di invadere un sito con un numero limitato di IP. La limitazione della velocità è particolarmente consigliata per proteggere gli URI che hanno costi o impatto elevati, come le pagine di accesso o di creazione di account.

Le regole di limitazione della velocità possono fornire un primo livello di difesa efficiente in termini di costi. Puoi utilizzare regole più avanzate per proteggere gli URI sensibili. Le regole basate sulla frequenza specifiche degli URI possono limitare l'impatto sulle pagine critiche o sulle API che influiscono sul backend, come l'accesso al database. Le mitigazioni avanzate per proteggere determinati URI, illustrate più avanti in questa guida, spesso comportano costi aggiuntivi e queste regole basate sulla tariffa specifiche per gli URI possono aiutarti a controllare i costi. Per ulteriori informazioni sulle regole basate sulla tariffa comunemente consigliate, consulta Le tre regole basate sulla tariffa più importanti nel Security Blog. AWS WAF AWS In alcune situazioni, è utile limitare il tipo di richiesta valutata da una regola basata sulla tariffa. È possibile utilizzare le istruzioni scope-down per, ad esempio, limitare le regole basate sulla frequenza in base all'area geografica dell'indirizzo IP di origine.

AWS WAF offre una funzionalità avanzata per le regole basate sulla velocità tramite l'uso di chiavi di aggregazione. Con questa funzionalità, è possibile configurare una regola basata sulla frequenza per utilizzare varie altre chiavi di aggregazione e combinazioni di tasti, oltre all'indirizzo IP di origine. Ad esempio, come singola combinazione, puoi aggregare le richieste in base a un indirizzo IP inoltrato, al metodo HTTP e a un argomento di query. Ciò consente di configurare regole più dettagliate per una sofisticata mitigazione del traffico volumetrico.

Controlli intrinseci

I controlli intrinseci sono vari tipi di convalide o verifiche interne o intrinseche all'interno di un sistema o processo. Per il controllo dei bot, AWS WAF esegue un controllo intrinseco convalidando che le informazioni inviate nella richiesta corrispondano ai segnali del sistema. Ad esempio, esegue ricerche DNS inverse e altre verifiche di sistema. Alcune richieste automatiche sono necessarie, come le richieste relative alla SEO. L'opzione Allow Listing è un modo per consentire l'accesso a bot validi e attesi. A volte, però, i bot malevoli emulano bot validi e può essere difficile separarli. AWS WAF fornisce metodi per eseguire questa operazione tramite il gruppo di regole AWS WAF Bot Control gestito. Le regole di questo gruppo consentono di verificare che i bot autoidentificati siano chi dicono

di essere. AWS WAF verifica i dettagli della richiesta rispetto allo schema noto di quel bot ed esegue anche ricerche DNS inverse e altre verifiche oggettive.

Controlli di identificazione dei client per la gestione dei bot

Se il traffico correlato agli attacchi non può essere facilmente riconosciuto tramite attributi statici, il rilevamento deve essere in grado di identificare con precisione il client che effettua la richiesta. Ad esempio, le regole basate sulla frequenza sono spesso più efficaci e più difficili da eludere quando l'attributo a cui è limitato la frequenza è specifico dell'applicazione, come un cookie o un token. L'utilizzo di un cookie legato a una sessione impedisce agli operatori di botnet di duplicare flussi di richieste simili su molti bot.

L'acquisizione di token viene comunemente utilizzata per l'identificazione dei clienti. Per l'acquisizione di token, un JavaScript codice raccoglie informazioni per generare un token che viene valutato sul lato server. La valutazione può variare dalla verifica che JavaScript sia in esecuzione sul client alla raccolta di informazioni sul dispositivo per il rilevamento delle impronte digitali. L'acquisizione di token richiede l'integrazione di un JavaScript SDK nel sito o nell'applicazione oppure richiede che un fornitore di servizi esegua l'iniezione in modo dinamico.

La richiesta di JavaScript supporto aggiunge un ulteriore ostacolo per i bot che tentano di emulare i browser. Quando è coinvolto un SDK, ad esempio in un'applicazione mobile, l'acquisizione di token verifica l'implementazione dell'SDK e impedisce ai bot di imitare le richieste dell'applicazione.

L'acquisizione di token richiede l'uso di SDK implementati sul lato client della connessione. Le seguenti AWS WAF funzionalità forniscono un SDK JavaScript basato su browser e un SDK basato su applicazioni per dispositivi mobili: Bot Control, Fraud Control Account Takeover Prevention (ATP) e Fraud Control per la creazione di account (ACFP).

Le tecniche per l'identificazione dei clienti includono CAPTCHA, profilazione del browser, impronta digitale del dispositivo e impronta digitale TLS.

CAPTCHA

Il test di Turing pubblico completamente automatizzato per distinguere computer e umani (CAPTCHA) viene utilizzato per distinguere tra visitatori robotici e umani e per prevenire il web scraping, il furto di credenziali e lo spam. Esistono diverse implementazioni, ma spesso implicano un enigma che un essere umano può risolvere. I CAPTCHA offrono un ulteriore livello di difesa contro i bot comuni e possono ridurre i falsi positivi nel rilevamento dei bot.

AWS WAF consente alle regole di eseguire un'azione CAPTCHA contro le richieste web che soddisfano i criteri di ispezione di una regola. Questa azione è il risultato della valutazione delle informazioni di identificazione del cliente raccolte dal servizio. AWS WAF le regole possono richiedere la risoluzione dei problemi relativi al CAPTCHA per risorse specifiche che sono spesso prese di mira dai bot, come il login, la ricerca e l'invio di moduli. AWS WAF possono servire direttamente CAPTCHA tramite mezzi interstiziali o utilizzando un SDK per gestirlo sul lato client. Per ulteriori informazioni, consulta CAPTCHA e Challenge in. AWS WAF

Profilazione del browser

La profilazione del browser è un metodo di raccolta e valutazione delle caratteristiche del browser, nell'ambito dell'acquisizione di token, per distinguere gli esseri umani reali che utilizzano un browser interattivo dall'attività distribuita dei bot. È possibile eseguire la profilazione del browser in modo passivo tramite intestazioni, ordine delle intestazioni e altre caratteristiche delle richieste inerenti al funzionamento dei browser.

È inoltre possibile eseguire la profilazione del browser nel codice utilizzando l'acquisizione di token. Utilizzando JavaScript per la profilazione del browser, è possibile determinare rapidamente se un client supporta. JavaScript Questo ti aiuta a rilevare bot semplici che non lo supportano. La profilazione del browser non controlla solo le intestazioni HTTP e il JavaScript supporto; la profilazione del browser rende difficile per i bot emulare completamente un browser web. Entrambe le opzioni di profilazione del browser hanno lo stesso obiettivo: trovare modelli in un profilo del browser che indichino un'incoerenza con il comportamento di un browser reale.

AWS WAF il controllo dei bot mirati indica, nell'ambito della valutazione dei token, se un browser mostra segni di automazione o segnali incoerenti. AWS WAF contrassegna la richiesta per eseguire l'azione specificata nella regola. Per ulteriori informazioni, consulta Rilevare e bloccare il traffico bot avanzato nel AWS Security Blog.

Impronta digitale del dispositivo

L'impronta digitale del dispositivo è simile alla profilazione del browser, ma non si limita ai browser. Il codice in esecuzione su un dispositivo (che può essere un dispositivo mobile o un browser Web) raccoglie e riporta i dettagli del dispositivo a un server di backend. I dettagli possono includere attributi di sistema, come memoria, tipo di CPU, tipo di kernel del sistema operativo (OS), versione del sistema operativo e virtualizzazione.

È possibile utilizzare l'impronta digitale del dispositivo per riconoscere se un bot sta emulando un ambiente o se vi sono segnali diretti che l'automazione è in uso. Oltre a ciò, l'impronta digitale del dispositivo può essere utilizzata anche per riconoscere le richieste ripetute dallo stesso dispositivo.

Il riconoscimento delle richieste ripetute dallo stesso dispositivo, anche se il dispositivo tenta di modificare alcune caratteristiche della richiesta, consente a un sistema di backend di imporre regole di limitazione della velocità. Le regole di limitazione della velocità basate sull'impronta digitale del dispositivo sono in genere più efficaci delle regole di limitazione della velocità basate sugli indirizzi IP. Questo ti aiuta a mitigare il traffico bot che ruota tra VPN o proxy ma proviene da un numero limitato di dispositivi.

Se utilizzato con gli SDK di integrazione delle applicazioni, il controllo tramite AWS WAF bot mirati può aggregare il comportamento delle richieste di sessione del client. Ciò consente di rilevare e separare le sessioni client legittime da quelle dannose, anche quando entrambe provengono dallo stesso indirizzo IP. Per ulteriori informazioni sul controllo dei AWS WAF bot mirati, consulta Rilevare e bloccare il traffico bot avanzato nel AWS Security Blog.

Impronta digitale TLS

Il fingerprinting TLS, noto anche come regole basate sulla firma, viene comunemente utilizzato quando i bot provengono da molti indirizzi IP ma presentano caratteristiche simili. Quando si utilizza HTTPS, i lati client e server si scambiano messaggi per confermarsi e verificarsi a vicenda. Stabiliscono algoritmi crittografici e chiavi di sessione. Questo è chiamato handshake TLS. Il modo in cui viene implementato un handshake TLS è una firma spesso utile per riconoscere attacchi di grandi dimensioni distribuiti su molti indirizzi IP.

L'impronta digitale TLS consente ai server Web di determinare l'identità di un client Web con un elevato grado di precisione. Richiede solo i parametri della prima connessione a pacchetto, prima che avvenga lo scambio di dati dell'applicazione. In questo caso, il client Web si riferisce all'applicazione che avvia una richiesta, che potrebbe essere un browser, uno strumento CLI, uno script (bot), un'applicazione nativa o un altro client.

Un approccio di impronta digitale SSL e TLS è l'impronta digitale JA3. JA3 rileva le impronte digitali di una connessione client in base ai campi del messaggio Client Hello dell'handshake SSL o TLS. Ti aiuta a profilare client SSL e TLS specifici su diversi indirizzi IP di origine, porte e certificati X.509.

Amazon CloudFront supporta l'aggiunta di intestazioni JA3 alle richieste. Un'`CloudFront-Viewer-JA3-Fingerprint`intestazione contiene un'impronta digitale hash a 32 caratteri del pacchetto TLS Client Hello di una richiesta di visualizzazione in entrata. L'impronta digitale incapsula le

informazioni su come comunica il client. Queste informazioni possono essere utilizzate per profilare i clienti che condividono lo stesso modello. È possibile aggiungere l'`CloudFront-Viewer-JA3-Fingerprint`intestazione a una policy di richiesta di origine e allegare la politica a una CloudFront distribuzione. Puoi quindi controllare il valore dell'intestazione nelle applicazioni di origine o in Lambda @Edge and Functions. CloudFront Puoi confrontare il valore dell'intestazione con un elenco di impronte digitali di malware note per bloccare i client dannosi. Puoi anche confrontare il valore dell'intestazione con un elenco di impronte digitali previste per consentire le richieste solo da client noti.

Controlli di analisi avanzati per la gestione dei bot

Alcuni bot utilizzano strumenti di inganno avanzati per eludere attivamente il rilevamento. Questi bot imitano il comportamento umano per svolgere un'attività specifica, come lo scalping. Questi bot hanno uno scopo e di solito è collegato a una grande ricompensa monetaria.

Questi bot avanzati e persistenti utilizzano un mix di tecnologie per eludere il rilevamento o confondersi con il traffico normale. A sua volta, ciò richiede anche una combinazione di diverse tecnologie di rilevamento per identificare e mitigare con precisione il traffico dannoso.

Casi d'uso mirati

I dati relativi ai casi d'uso possono offrire opportunità di rilevamento dei bot. I rilevamenti di frodi sono casi d'uso speciali in cui è necessaria una mitigazione speciale. Ad esempio, per prevenire l'acquisizione di account, puoi confrontare un elenco di nomi utente e password di account compromessi con le richieste di accesso o di creazione di account. Ciò consente ai proprietari di siti Web di rilevare i tentativi di accesso che utilizzano credenziali compromesse. L'uso di credenziali compromesse può indicare che i bot stanno tentando di impadronirsi di un account, oppure potrebbe trattarsi di utenti che non sanno che le proprie credenziali sono state compromesse. In questo caso d'uso, i proprietari di siti Web possono adottare ulteriori misure per verificare l'utente e quindi aiutarlo a modificare la password. AWS WAF fornisce la regola gestita per la prevenzione delle acquisizioni di account (ATP) di Fraud Control per questo caso d'uso.

Rilevamento di bot a livello di applicazione o aggregato

Alcuni casi d'uso richiedono la combinazione dei dati sulle richieste provenienti dalla rete di distribuzione dei contenuti (CDN) e dal backend dell'applicazione o del servizio. AWS WAF A volte, è persino necessario integrare l'intelligence di terze parti per poter prendere decisioni affidabili sui bot.

Funziona in Amazon CloudFront e AWS WAF può inviare segnali all'infrastruttura di backend oppure può successivamente aggregare le regole tramite intestazioni ed etichette. CloudFront espone le intestazioni di impronte digitali JA3, come accennato in precedenza. Questo è un esempio di CloudFront fornitura di tali dati tramite un'intestazione. AWS WAF può inviare etichette quando corrisponde a una regola. Le regole successive possono utilizzare queste etichette per prendere decisioni migliori sui bot. Quando si combinano più regole, è possibile implementare controlli altamente granulari. Un caso d'uso comune consiste nell'abbinare parti di una regola gestita tramite un'etichetta e quindi combinarla con altri dati di richiesta. Per ulteriori informazioni, consulta Esempi di abbinamento delle etichette nella AWS WAF documentazione.

Analisi dell'apprendimento automatico

Il machine leaning (ML) è una tecnica potente per gestire i bot. L'apprendimento automatico può adattarsi ai cambiamenti dei dettagli e, se combinato con altri strumenti, offre il modo più affidabile e completo per mitigare i bot con un numero minimo di falsi positivi. Le due tecniche di machine learning più comuni sono l'analisi comportamentale e il rilevamento delle anomalie. Con l'analisi comportamentale, un sistema (nel client, nel server o in entrambi) monitora il modo in cui un utente interagisce con l'applicazione o il sito Web. Monitora i modelli di movimento del mouse o la frequenza delle interazioni con clic e tocco. Il comportamento viene quindi analizzato con un modello ML per riconoscere i bot. Il rilevamento delle anomalie è simile. Si concentra sul rilevamento di comportamenti o modelli significativamente diversi da una linea di base definita per l'applicazione o il sito Web.

AWS WAF i controlli mirati per i bot forniscono una tecnologia ML predittiva. Questa tecnologia aiuta a difendersi dagli attacchi distribuiti basati su proxy, realizzati da bot progettati per eludere il rilevamento. Il gruppo di regole gestito di AWS WAF Bot Control utilizza l'analisi automatica e ML delle statistiche sul traffico del sito Web per rilevare comportamenti anomali indicativi di un'attività distribuita e coordinata dei bot.

Implementazione e implementazione della tua strategia di controllo dei bot

Esistono diversi fattori da considerare quando si pianifica una strategia di implementazione per il controllo dei bot. Oltre alle caratteristiche uniche delle applicazioni Web, le dimensioni dell'ambiente, il processo di sviluppo e la struttura organizzativa influiscono sulla strategia di implementazione. A seconda delle caratteristiche dell'ambiente e dell'applicazione, è possibile utilizzare una strategia di distribuzione centralizzata o decentralizzata:

- Strategia di implementazione centralizzata: un approccio centralizzato consente un livello di controllo più elevato quando si desidera un'applicazione rigorosa del controllo dei bot. Questo approccio è ideale se i team addetti alle applicazioni preferiscono affidare la gestione del carico. Un approccio centralizzato è più efficace quando le applicazioni Web condividono caratteristiche simili. In questo caso, le applicazioni traggono vantaggio da un insieme comune di regole di controllo dei bot e azioni di mitigazione dei bot.
- Strategia di implementazione decentralizzata: un approccio decentralizzato offre ai team delle applicazioni l'autonomia necessaria per definire e implementare le configurazioni di controllo dei bot in modo indipendente. Questo approccio è comune per gli ambienti più piccoli o quando i team applicativi devono mantenere il controllo sulle proprie politiche di controllo dei bot. A causa della natura di molte applicazioni Web, è spesso necessario mantenere politiche di controllo dei bot indipendenti e personalizzate in base alle caratteristiche uniche dell'applicazione, con il risultato di un approccio decentralizzato.
- Strategia combinata: una combinazione di questi due approcci è appropriata per una combinazione di applicazioni web. Ad esempio, ciò potrebbe comportare una serie di regole di base che si applicano a tutti gli ACL Web, mentre la gestione di policy di controllo dei bot più specifiche è delegata ai team applicativi.

È possibile utilizzarlo AWS Firewall Managerper centralizzare e automatizzare la distribuzione degli ACL AWS WAF Web che definiscono le politiche di controllo dei bot. Quando usi Firewall Manager, valuta se sia opportuno centralizzare le policy di controllo dei bot, anche se debbano essere delegate ai team applicativi. Con Firewall Manager, puoi utilizzare i tag per consentire ai team delle applicazioni di aderire alle politiche. AWS WAF Ciò fornisce funzionalità intelligenti AWS WAF di mitigazione delle minacce. È inoltre possibile abilitare la AWS WAF registrazione centralizzata per le applicazioni e le operazioni di sicurezza.

Indipendentemente dalla strategia di implementazione utilizzata, si consiglia di definire e gestire il processo di onboarding tramite framework basati su Infrastructure as Code (IaC), come o. AWS CloudFormationAWS Cloud Development Kit (AWS CDK) Ciò consente di configurare il controllo del codice sorgente per archiviare e modificare gli oggetti di configurazione. Per ulteriori informazioni, consultate gli esempi di AWS WAF configurazione per AWS CDK(GitHub) e CloudFormation(AWS documentazione).

Strategia di implementazione

Dopo aver selezionato una strategia di distribuzione, l'implementazione può iniziare. La strategia di distribuzione definisce il modo in cui le regole vengono implementate nelle diverse applicazioni. Nella strategia di implementazione, l'attenzione si concentra sul processo iterativo di aggiunta di controlli, test, monitoraggio continuo e valutazione dei relativi effetti.

Comprensione dei modelli di traffico

Per comprendere realmente i modelli di traffico, è importante acquisire familiarità con la funzione aziendale dell'applicazione e gli attributi previsti, come i modelli di utilizzo, le risorse chiave e i personaggi degli utenti. Incorporate il traffico di produzione e il traffico generato durante i test rispetto all'applicazione per stabilire una base per la valutazione. Assicurati che l'intervallo di tempo includa dati sul traffico che rappresentino sufficientemente i picchi di utilizzo multipli.

Utilizzando il tuo strumento preferito, esamina i registri di traffico e le metriche relative al periodo di utilizzo rappresentativo. Analizza i dati di AWS WAF registro alla ricerca di richieste anomale filtrando i campi di registro come `headers` (ad esempio, `User-Agent` e), e`Referer`. `country` `clientIp` Prendi nota degli Uniform Resource Identifier (URI) e della relativa frequenza di accesso. Categorizza il traffico, ad esempio identificando bot validi. Ad esempio, consenti l'accesso a bot utili, come i crawler e i monitor dei motori di ricerca.

Nella AWS WAF console, nella dashboard di controllo dei bot, è disponibile un esempio dell'attività dei bot per qualsiasi ACL web attivo. Sebbene ciò fornisca una prospettiva iniziale dei volumi di richieste dei bot più comuni, esegui ulteriori configurazioni e analisi per comprendere meglio l'attività dei bot.

Per un'implementazione efficace, è necessario conoscere bene il traffico dei bot, i suoi effetti e quali richieste dei bot sono vantaggiose rispetto a quelle dannose. Questo aiuta nella fase successiva, nella selezione dei controlli, e ti aiuta a valutare il traffico dei bot in parallelo.

Selezione e aggiunta di controlli

L'analisi iniziale del traffico aiuta a determinare quali controlli bot utilizzare e quali azioni selezionare per ciascuno di essi. Potresti anche scegliere di registrare e monitorare l'attività per potenziali azioni future. L'analisi iniziale del traffico ti aiuta a selezionare il controllo migliore per gestire il traffico. Per ulteriori informazioni sui controlli disponibili, Tecniche per il controllo dei bot consulta questa guida.

Valuta la possibilità di includere implementazioni SDK aggiuntive durante questa fase. Questo ti aiuta a testare e completare le implementazioni SDK in tutte le applicazioni richieste. AWS WAF Le regole di controllo dei bot e di controllo delle frodi offrono un vantaggio completo in termini di valutazione dei token quando si implementa JavaScript SDK o SDK per dispositivi mobili. Per ulteriori informazioni, consulta Perché utilizzare gli SDK di integrazione delle applicazioni con Bot Control nella documentazione. AWS WAF

Consigliamo di implementare l'acquisizione di token per diversi tipi di applicazioni come segue:

- Applicazione a pagina singola (SPA) — JavaScript SDK (nessun reindirizzamento)
- Browser mobile: JavaScript SDK o azioni relative alle regole (CAPTCHA o Challenge)
- Visualizzazioni Web: JavaScript SDK o azioni relative alle regole (CAPTCHA o Challenge)
- Applicazioni native: SDK per dispositivi mobili
- iFrames — SDK JavaScript

Per ulteriori informazioni su come implementare gli SDK, consulta l'integrazione delle applicazioni AWS WAF client nella documentazione. AWS WAF

Test e implementazione in produzione

I controlli devono essere inizialmente distribuiti in un ambiente non di produzione in cui sia possibile eseguire test per verificare che venga preservata la funzionalità prevista dell'applicazione Web. Eseguite sempre una convalida completa in un ambiente di test prima dell'implementazione in produzione.

Dopo il test e la convalida in un ambiente non di produzione, è possibile procedere con la release di produzione. Seleziona una data e un'ora con il traffico utente più basso previsto. Prima dell'implementazione, i team addetti alle applicazioni e alla sicurezza devono verificare la prontezza operativa, discutere su come ripristinare le modifiche e rivedere i dashboard per garantire che tutte le metriche e gli allarmi richiesti siano configurati.

Con la distribuzione CloudFront continua di Amazon, puoi inviare una piccola quantità di traffico a una distribuzione temporanea con un ACL AWS WAF Web configurato specificamente per la valutazione del controllo dei bot. AWS WAF fornisce la gestione delle versioni di qualsiasi regola gestita nuova o aggiornata in modo da poter testare e approvare le modifiche prima che inizino a valutare il traffico di produzione.

Valutazione e ottimizzazione dei controlli

I controlli implementati possono fornire ulteriori informazioni e visibilità sull'attività e sui modelli di traffico. Monitora e analizza frequentemente il traffico delle applicazioni per aggiungere o modificare i controlli di sicurezza. Normalmente è prevista una fase di ottimizzazione per mitigare potenziali falsi negativi e falsi positivi. I falsi negativi sono attacchi che non sono stati rilevati dai controlli dell'utente e che richiedono l'irrigidimento delle regole. I falsi positivi rappresentano richieste legittime che sono state erroneamente identificate come attacchi e di conseguenza bloccate.

L'analisi e la regolazione possono essere eseguite manualmente o con l'ausilio di strumenti. Un sistema SIEM (Security Information and Event Management) è uno strumento comune che aiuta a fornire metriche e monitoraggio intelligente. Ce ne sono molti disponibili con diversi gradi di sofisticazione, ma tutti forniscono un buon punto di partenza per ottenere informazioni sul traffico.

La definizione di importanti indicatori chiave di prestazione (KPI) per siti Web e applicazioni può aiutarvi a identificare più rapidamente quando le cose non funzionano come previsto. Ad esempio, è possibile utilizzare gli addebiti sulle carte di credito, le vendite per account o i tassi di conversione come indicatori delle anomalie aziendali che possono essere generate dai bot. Definire e comprendere quali metriche e KPI è importante monitorare è ancora più importante del semplice monitoraggio.

Capire come ottenere le metriche e i log corretti da una soluzione di controllo dei bot è tanto importante quanto identificare le metriche da monitorare. La sezione successiva descrive in dettaglio Linee guida per il monitoraggio della strategia di controllo dei bot le opzioni di monitoraggio e visibilità da considerare.

Linee guida per il monitoraggio della strategia di controllo dei bot

Per il traffico dei bot e il traffico delle applicazioni web, il monitoraggio e la visibilità sono di grande importanza. Ti aiuta a dare priorità alle attività e alle operazioni di sicurezza. Se la registrazione dettagliata o l'utilizzo di un sistema SIEM non sono possibili, un buon punto di partenza è il monitoraggio delle metriche di base fornite dalla soluzione o dal fornitore selezionato.

Questa visibilità è utile per l'intelligence sulle minacce, il rafforzamento delle regole, la risoluzione dei falsi positivi e la risposta a un incidente. Sono disponibili diverse opzioni di monitoraggio con. AWS WAF Per un monitoraggio di alto livello, AWS WAF fornisce informazioni sulla panoramica del traffico in. AWS Management ConsoleÈ disponibile per tutto il traffico e per una visualizzazione dettagliata per il traffico dei bot, quando il gruppo di regole Bot Control è abilitato nell'ACL web.

AWS WAF offre diverse opzioni per la registrazione dettagliata del traffico ACL web. È inoltre possibile aggiungere etichette alle richieste, che è possibile utilizzare per facilitare l'analisi dei log e configurare le regole di valutazione dei bot. Integrando Amazon CloudWatch Logs Insights, puoi interrogare AWS WAF i log e visualizzare i risultati.

Se attivi la registrazione dettagliata, AWS WAF offre una visibilità aggiuntiva oltre alla dashboard di controllo dei bot preconfigurata. L'utilizzo AWS WAF dei log per visualizzare il traffico, nonché di indagini ad hoc, può fornire una comprensione approfondita dei modelli di traffico e delle opzioni di mitigazione per un'applicazione web.

Puoi integrare i dati di AWS WAF log con Amazon CloudWatch Logs, Amazon Simple Storage Service (Amazon S3) o Amazon Data Firehose. Per ulteriori informazioni, consulta AWS WAF Attivare la registrazione e inviare log a CloudWatch, Amazon S3 o Amazon Data Firehose. Puoi anche inviare log a vari obiettivi per l'analisi, tra cui Amazon OpenSearch Service o una Marketplace AWSsoluzione. Per ulteriori informazioni, vedere Impostazioni di destinazione nella documentazione di Firehose. Se vengono utilizzate più fonti di registro, si consiglia una soluzione di registrazione centralizzata per correlare le fonti.

Successivamente, questa guida fornisce consigli su come iniziare a monitorare il traffico dei bot e ottenere visibilità utilizzando Amazon CloudWatch.

Monitoraggio delle regole principali

Il monitoraggio delle regole più importanti può evidenziare tendenze e attività potenzialmente anomale. L'aumento delle percentuali relative a una regola specifica potrebbe indicare una potenziale attività mirata o falsa positiva su cui dovresti indagare. La regola più comune per il tracciamento sarebbero Controlli basati su IP le regole di blocco geografico (un picco in questo caso può mostrare traffico proveniente da paesi insoliti, che potrebbe non essere bloccato automaticamente) e. Regole basata sulla frequenza Queste regole avrebbero sempre delle variazioni intrinseche, ma un'anomalia nel modello di traffico può essere indicativa dell'attività dei bot. Tienilo in considerazione se imposti manualmente le soglie.

Monitoraggio delle etichette e dei namespace principali

Utilizzando le CloudWatch metriche per tenere traccia delle etichette principali, puoi vedere quali AWS WAF regole vengono richiamate di frequente. Questo ti aiuta a rilevare anomalie, come un aumento dell'attività dello scraper, il traffico proveniente da fonti sospette o il tentativo di abuso della pagina di accesso dell'applicazione o dell'API.

Di seguito sono riportati alcuni esempi di etichette che potrebbero interessarti:

- `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`

Di seguito sono riportati alcuni esempi di namespace di etichette che potrebbero interessarti:

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

Creazione di espressioni matematiche

In Amazon CloudWatch, puoi creare espressioni matematiche per una o tutte le regole. Se imposti avvisi sulle espressioni matematiche, riceverai notifiche relative alle anomalie nelle tariffe, non nelle quantità, di determinate metriche. Si tratta di uno strumento importante per ridurre l'affaticamento dovuto all'allerta.

Crea una metrica personalizzata basata su un'espressione matematica. Guarda le tariffe relative per le regole, rispetto al numero complessivo di richieste a un'applicazione. Quella che segue è un'espressione matematica comune:

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

Questa espressione matematica fornisce una percentuale che consente di tenere traccia di una regola specifica e visualizzarne l'andamento nel tempo.

Utilizzo del rilevamento delle anomalie

L'utilizzo del rilevamento delle CloudWatch anomalie su qualsiasi CloudWatch metrica può fornire avvisi su tendenze anormalmente basse o alte, senza impostare manualmente la soglia effettiva. Questi algoritmi analizzano continuamente le metriche di sistemi e applicazioni, determinano le linee di base normali e le anomalie riscontrate con un intervento minimo da parte dell'utente. CloudWatch applica algoritmi statistici e ML nella sua funzione di rilevamento delle anomalie.

Utilizzo dei CloudWatch parametri di Amazon

AWS WAF elabora il traffico e aggiunge etichette alle richieste che corrispondono alle regole definite nell'ACL web. Ogni etichetta crea una metrica in. CloudWatch Allo stesso tempo, ogni regola ACL web crea anche metriche per ciascuna delle sue azioni possibili. Utilizza queste metriche di etichette e azioni per acquisire una comprensione di alto livello del traffico dei bot. Si tratta di un approccio conveniente per visualizzare le tendenze. Per ulteriori informazioni, consulta Visualizza le metriche disponibili e le metriche grafiche nella documentazione. CloudWatch

CloudWatch offre la possibilità di inviare dati a un raccoglitore o aggregatore di log, sia esso una soluzione o una Servizio AWS soluzione di terze parti. L'acquisizione di dati da CloudWatch può fornire un'esperienza di osservabilità della sicurezza più consolidata, in cui è possibile correlare i dati provenienti da più fonti. Questo può aiutarti a esaminare, visualizzare o configurare gli avvisi e le automazioni di sicurezza.

Creazione di una dashboard

Dopo aver identificato le metriche importanti da monitorare, crea una dashboard che contenga le metriche più pertinenti. Visualizzarle side-by-side, sotto un unico pannello di vetro, può fornire visibilità e controllo aggiuntivi.

È sempre preferibile configurare avvisi e regole di automazione per valori metrici anomali. Non affidatevi agli esseri umani per identificare le anomalie guardando una dashboard. Tuttavia, i dashboard possono essere utili per scopi di indagine dopo la ricezione di un avviso.

Ottimizzazione dei costi per la tua strategia di controllo dei bot

La natura del traffico web è dinamica. Ciò significa che la tecnologia e i servizi utilizzati per mitigare le minacce possono variare ed essere ottimizzati nel tempo. Questo è fondamentale quando si considera una strategia di controllo dei bot e i controlli inclusi in essa. L'ottimizzazione nel tempo è il principio principale da tenere a mente e deriva dal pilastro dell'ottimizzazione dei costi del AWS Well-Architected Framework.

AWS WAF Gli ACL web possono essere dinamici, soprattutto quando vengono rilasciate nuove funzionalità o si sta cercando di mitigare una nuova minaccia. Tenere d'occhio i costi implica comprendere le dimensioni di costo del AWS WAF servizio e il modo in cui ciascuna di esse influisce sulla spesa finale. Il principale costo determinante è il numero di richieste valutate dal servizio. Sono previsti costi aggiuntivi se utilizzi i gruppi di regole gestiti da Bot Control e Account Takeover Prevention (ATP) o se utilizzi azioni avanzate, come CAPTCHA o challenge.

Poiché i controlli specializzati dei bot hanno un costo elevato, l'obiettivo principale di ottimizzazione dei costi è ridurre il numero di richieste esaminate da questi controlli avanzati. Le tecniche applicabili includono la separazione dei contenuti di alto valore, l'applicazione innanzitutto di misure a basso costo, la definizione dell'area di valutazione e la combinazione della protezione dei bot con altri tipi di controlli. Le tecniche di monitoraggio dei costi forniscono ulteriore visibilità all'interno dell'organizzazione.

Separazione dei contenuti dinamici e statici

Una tecnica di riduzione dei costi consiste nell'isolare il contenuto statico dall'applicazione dinamica. La maggior parte delle richieste alle applicazioni Web tipiche riguarda oggetti statici. Un metodo comune per ridurre il carico sui server delle applicazioni consiste nello spostare il contenuto statico nel proprio URL, ad esempio`static.example.com`. Ciò si ottiene spesso creando una distribuzione unica per la distribuzione dei contenuti con la configurazione di memorizzazione nella cache ottimizzata per i contenuti statici. Questa tecnica può anche aiutare a ridurre i costi di controllo dei bot se il contenuto statico non è comunemente preso di mira nel sito o nell'applicazione. La separazione del contenuto statico dall'applicazione dinamica può consentire un'applicazione più precisa dei controlli avanzati dei bot.

Applicare innanzitutto regole a basso costo

Un'altra tecnica consiste nell'applicare regole di base a basso costo che filtrino il traffico indesiderato prima di utilizzare i controlli avanzati, che sono più costosi. In pratica, ciò significa in genere utilizzare le mitigazioni del controllo dei bot come ultimo livello di difesa e utilizzare i controlli precedenti per filtrare il traffico indesiderato. Questo approccio piramidale è stato discusso in precedenza Tecniche per il controllo dei bot in questa guida. L'obiettivo principale è utilizzare queste opzioni a basso costo per bloccare il traffico indesiderato, riducendo così il numero di richieste elaborate con tecniche di mitigazione avanzate e più costose.

Analisi dettagliata dell'area di valutazione

AWS WAFle istruzioni scope-down forniscono una tecnica potente per ridurre il numero di richieste esaminate da regole avanzate. Se non è possibile implementare la separazione del contenuto statico in un proprio URL, le istruzioni scope-down sono un altro metodo per filtrare le richieste che non richiedono tecniche di mitigazione avanzate. Ciò può essere fatto definendo un percorso specifico dell'applicazione, un metodo HTTP (come POST) o una combinazione simile.

Combinare la protezione dai bot con altri controlli

Quando si proteggono le applicazioni da molteplici minacce oltre al traffico di bot indesiderato, è necessario prendere in considerazione ulteriori considerazioni relative al controllo dei costi. Ad esempio, la protezione dagli attacchi DDoS (Distributed Denial of Service) e dall'acquisizione di account richiede una configurazione aggiuntiva che può influire sui costi. Shield Advanced è consigliato per proteggere le applicazioni dagli attacchi DDoS. In particolare, le sue mitigazioni a livello di applicazione possono risolvere automaticamente i flussi di richieste, riducendo così il numero di richieste che possono essere elaborate dal gruppo di regole AWS WAF Bot Control, quando la regola viene inserita in primo piano nell'ordine di valutazione. Shield Advanced offre un ulteriore vantaggio: AWS WAF le regole standard gestite e personalizzate non comportano costi aggiuntivi per le risorse protette da Shield Advanced. Tieni presente che i gruppi di regole intelligenti per la mitigazione delle minacce, incluso Bot Control, comportano costi aggiuntivi, anche per le risorse protette da Shield Advanced.

Le applicazioni che richiedono la prevenzione dell'acquisizione di account possono utilizzare il gruppo di regole ATP (Account Takeover Prevention) di AWS WAF Fraud Control. Il costo di ispezione per richiesta del gruppo di regole ATP è superiore a quello del gruppo di regole Bot Control. Questo costo più elevato rende fondamentale applicare il gruppo di regole ATP nel modo più preciso possibile.

L'utilizzo del gruppo di regole Bot Control insieme all'ATP può contribuire a raggiungere questo obiettivo. Il gruppo di regole Bot Control deve essere anteposto all'ATP nell'ACL web per filtrare le richieste dei bot e ridurre il numero di richieste ispezionate dall'ATP.

Per l'ottimizzazione continua, l'attività più importante è il monitoraggio delle CloudWatchmetriche associate al gruppo di regole Bot Control. L'obiettivo, nel tempo, è ridurre il numero di richieste valutate dal gruppo di regole Bot Control alle sole richieste che riguardano le risorse necessarie per proteggere dalle attività indesiderate dei bot. La creazione di CloudWatch dashboard offre la visibilità delle metriche più importanti per le applicazioni, inclusi AWS WAF costi e utilizzo.

Monitoraggio dei costi

AWS Cost Explorer è uno strumento che permette di visualizzare e analizzare i costi e l'utilizzo. Cost Explorer facilita l'analisi dei AWS costi, compresi AWS WAF i costi sostenuti. Lo strumento fornisce informazioni sui costi per gli ultimi 12 mesi e prevede le spese future per i prossimi 12 mesi.

AWS Cost Anomaly Detection è un altro strumento di controllo della gestione dei costi che può essere utile per monitorare AWS WAF i costi. Utilizza tecnologie ML avanzate per identificare le spese anomale e le cause principali. In questo modo è possibile intervenire rapidamente o ricevere avvisi in caso di aumento imprevisto dei costi. Ricevere un avviso quando viene raggiunta una soglia di costo specifica, Budget AWSpuò fornire tale funzionalità di tracciamento e monitoraggio.

Risorse

AWS documentazione

- AWS WAF guida per sviluppatori
- AWS Best practice per la resilienza agli attacchi DDoS (white paper)AWS
- Linee guida per l'implementazione (white paper) AWS WAFAWS

Altre risorse AWS

- Analisi dei AWS WAF log in Amazon CloudWatch Logs (post sul blog)AWS
- Implementa una dashboard AWS WAF con il minimo sforzo (post sul blog)AWS
- Automazioni di sicurezza per AWS WAF (AWS Solutions Library)
- Le tre regole più importanti AWS WAF basate sulla tariffa (AWS post sul blog)
- Visualizza i AWS WAF log con una CloudWatch dashboard di Amazon (AWS post sul blog)

Collaboratori

Creazione

- Diana Alvarado, Senior Solutions Architect, AWS
- Cameron Worrell, architetto aziendale, AWS
- Geary Scherer, architetto delle soluzioni, AWS
- Tzoori Tamam, architetto principale delle soluzioni, AWS

Revisione

- Jess Izen, ingegnere senior per lo sviluppo software, AWS
- Kaustubh Phatak, Senior Product Manager, AWS
- Vikramaditya Bhatnagar, consulente senior per la sicurezza, AWS

Scrittura tecnica

- Lilly AbouHarb, scrittrice tecnica senior, AWS

Cronologia dei documenti

La tabella seguente descrive le modifiche significative apportate a questa guida. Per ricevere notifiche sugli aggiornamenti futuri, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Pubblicazione iniziale	—	21 febbraio 2024

AWS Glossario delle linee guida prescrittive

I seguenti sono termini di uso comune nelle strategie, nelle guide e nei modelli forniti da AWS Prescriptive Guidance. Per suggerire voci, utilizza il link Fornisci feedback alla fine del glossario.

Numeri

7 R

Sette strategie di migrazione comuni per trasferire le applicazioni sul cloud. Queste strategie si basano sulle 5 R identificate da Gartner nel 2011 e sono le seguenti:

- Rifattorizzare/riprogettare: trasferisci un'applicazione e modifica la sua architettura sfruttando appieno le funzionalità native del cloud per migliorare l'agilità, le prestazioni e la scalabilità. Ciò comporta in genere la portabilità del sistema operativo e del database. Esempio: migra il tuo database Oracle locale all'edizione compatibile con Amazon Aurora PostgreSQL.
- Ridefinire la piattaforma (lift and reshape): trasferisci un'applicazione nel cloud e introduci un certo livello di ottimizzazione per sfruttare le funzionalità del cloud. Esempio: migra il tuo database Oracle locale ad Amazon Relational Database Service (Amazon RDS) per Oracle in. Cloud AWS
- Riacquistare (drop and shop): passa a un prodotto diverso, in genere effettuando la transizione da una licenza tradizionale a un modello SaaS. Esempio: migra il tuo sistema di gestione delle relazioni con i clienti (CRM) su Salesforce.com.
- Eseguire il rehosting (lift and shift): trasferisci un'applicazione sul cloud senza apportare modifiche per sfruttare le funzionalità del cloud. Esempio: migra il database Oracle locale su Oracle su un'istanza in. EC2 Cloud AWS
- Trasferire (eseguire il rehosting a livello hypervisor): trasferisci l'infrastruttura sul cloud senza acquistare nuovo hardware, riscrivere le applicazioni o modificare le operazioni esistenti. Si esegue la migrazione dei server da una piattaforma locale a un servizio cloud per la stessa piattaforma. Esempio: migra un'applicazione suMicrosoft Hyper-V. AWS
- Riesaminare (mantenere): mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a un momento successivo e applicazioni legacy che desideri mantenere, perché non vi è alcuna giustificazione aziendale per effettuarne la migrazione.
- Ritirare: disattiva o rimuovi le applicazioni che non sono più necessarie nell'ambiente di origine.

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

Un metodo di migrazione del database in cui i database di origine e di destinazione vengono mantenuti sincronizzati (utilizzando uno strumento di replica bidirezionale o operazioni di doppia scrittura) ed entrambi i database gestiscono le transazioni provenienti dalle applicazioni di connessione durante la migrazione. Questo metodo supporta la migrazione in piccoli batch controllati anziché richiedere una conversione una tantum. È più flessibile ma richiede più lavoro rispetto alla migrazione attiva-passiva.

migrazione attiva-passiva

Un metodo di migrazione di database in cui i database di origine e di destinazione vengono mantenuti sincronizzati, ma solo il database di origine gestisce le transazioni provenienti dalle applicazioni di connessione mentre i dati vengono replicati nel database di destinazione. Il database di destinazione non accetta alcuna transazione durante la migrazione.

funzione aggregata

Una funzione SQL che opera su un gruppo di righe e calcola un singolo valore restituito per il gruppo. Esempi di funzioni aggregate includono `SUM` e. `MAX`

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

Il processo di eliminazione permanente delle informazioni personali in un set di dati. L'anonimizzazione può aiutare a proteggere la privacy personale. I dati anonimi non sono più considerati dati personali.

anti-modello

Una soluzione utilizzata di frequente per un problema ricorrente in cui la soluzione è controproducente, inefficace o meno efficace di un'alternativa.

controllo delle applicazioni

Un approccio alla sicurezza che consente l'uso solo di applicazioni approvate per proteggere un sistema dal malware.

portfolio di applicazioni

Una raccolta di informazioni dettagliate su ogni applicazione utilizzata da un'organizzazione, compresi i costi di creazione e manutenzione dell'applicazione e il relativo valore aziendale. Queste informazioni sono fondamentali per il processo di scoperta e analisi del portfolio e aiutano a identificare e ad assegnare la priorità alle applicazioni da migrare, modernizzare e ottimizzare.

intelligenza artificiale (IA)

Il campo dell'informatica dedicato all'uso delle tecnologie informatiche per svolgere funzioni cognitive tipicamente associate agli esseri umani, come l'apprendimento, la risoluzione di problemi e il riconoscimento di schemi. Per ulteriori informazioni, consulta la sezione Che cos'è l'intelligenza artificiale?

operazioni di intelligenza artificiale (AIOps)

Il processo di utilizzo delle tecniche di machine learning per risolvere problemi operativi, ridurre gli incidenti operativi e l'intervento umano e aumentare la qualità del servizio. Per ulteriori informazioni su come AIOps viene utilizzato nella strategia di AWS migrazione, consulta la guida all'integrazione delle operazioni.

crittografia asimmetrica

Un algoritmo di crittografia che utilizza una coppia di chiavi, una chiave pubblica per la crittografia e una chiave privata per la decrittografia. Puoi condividere la chiave pubblica perché non viene utilizzata per la decrittografia, ma l'accesso alla chiave privata deve essere altamente limitato.

atomicità, consistenza, isolamento, durabilità (ACID)

Un insieme di proprietà del software che garantiscono la validità dei dati e l'affidabilità operativa di un database, anche in caso di errori, interruzioni di corrente o altri problemi.

Controllo degli accessi basato su attributi (ABAC)

La pratica di creare autorizzazioni dettagliate basate su attributi utente, come reparto, ruolo professionale e nome del team. Per ulteriori informazioni, consulta ABAC AWS nella documentazione AWS Identity and Access Management (IAM).

fonte di dati autorevole

Una posizione in cui è archiviata la versione principale dei dati, considerata la fonte di informazioni più affidabile. È possibile copiare i dati dalla fonte di dati autorevole in altre posizioni allo scopo di elaborarli o modificarli, ad esempio anonimizzandoli, oscurandoli o pseudonimizzandoli.

Zona di disponibilità

Una posizione distinta all'interno di un edificio Regione AWS che è isolata dai guasti in altre zone di disponibilità e offre una connettività di rete economica e a bassa latenza verso altre zone di disponibilità nella stessa regione.

AWS Cloud Adoption Framework (CAF)AWS

Un framework di linee guida e best practice AWS per aiutare le organizzazioni a sviluppare un piano efficiente ed efficace per passare con successo al cloud. AWS CAF organizza le linee guida in sei aree di interesse chiamate prospettive: business, persone, governance, piattaforma, sicurezza e operazioni. Le prospettive relative ad azienda, persone e governance si concentrano sulle competenze e sui processi aziendali; le prospettive relative alla piattaforma, alla sicurezza e alle operazioni si concentrano sulle competenze e sui processi tecnici. Ad esempio, la prospettiva relativa alle persone si rivolge alle parti interessate che gestiscono le risorse umane (HR), le funzioni del personale e la gestione del personale. In questa prospettiva, AWS CAF fornisce linee guida per lo sviluppo delle persone, la formazione e le comunicazioni per aiutare a preparare l'organizzazione all'adozione del cloud di successo. Per ulteriori informazioni, consulta il sito web di AWS CAF e il white paper AWS CAF.

AWS Workload Qualification Framework (WQF)AWS

Uno strumento che valuta i carichi di lavoro di migrazione dei database, consiglia strategie di migrazione e fornisce stime del lavoro. AWS WQF è incluso in (). AWS Schema Conversion Tool AWS SCT Analizza gli schemi di database e gli oggetti di codice, il codice dell'applicazione, le dipendenze e le caratteristiche delle prestazioni e fornisce report di valutazione.

B

bot difettoso

Un bot che ha lo scopo di interrompere o causare danni a individui o organizzazioni.

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

Una vista unificata, interattiva dei comportamenti delle risorse e delle interazioni nel tempo. Puoi utilizzare un grafico comportamentale con Amazon Detective per esaminare tentativi di accesso non riusciti, chiamate API sospette e azioni simili. Per ulteriori informazioni, consulta Dati in un grafico comportamentale nella documentazione di Detective.

sistema big-endian

Un sistema che memorizza per primo il byte più importante. Vedi anche endianness.

Classificazione binaria

Un processo che prevede un risultato binario (una delle due classi possibili). Ad esempio, il modello di machine learning potrebbe dover prevedere problemi come "Questa e-mail è spam o non è spam?" o "Questo prodotto è un libro o un'auto?"

filtro Bloom

Una struttura di dati probabilistica ed efficiente in termini di memoria che viene utilizzata per verificare se un elemento fa parte di un set.

distribuzioni blu/verdi

Una strategia di implementazione in cui si creano due ambienti separati ma identici. La versione corrente dell'applicazione viene eseguita in un ambiente (blu) e la nuova versione dell'applicazione nell'altro ambiente (verde). Questa strategia consente di ripristinare rapidamente il sistema con un impatto minimo.

bot

Un'applicazione software che esegue attività automatizzate su Internet e simula l'attività o l'interazione umana. Alcuni bot sono utili o utili, come i web crawler che indicizzano le informazioni su Internet. Alcuni altri bot, noti come bot dannosi, hanno lo scopo di disturbare o causare danni a individui o organizzazioni.

botnet

Reti di bot infettate da malware e controllate da un'unica parte, nota come bot herder o bot operator. Le botnet sono il meccanismo più noto per scalare i bot e il loro impatto.

ramo

Un'area contenuta di un repository di codice. Il primo ramo creato in un repository è il ramo principale. È possibile creare un nuovo ramo a partire da un ramo esistente e quindi sviluppare funzionalità o correggere bug al suo interno. Un ramo creato per sviluppare una funzionalità viene comunemente detto ramo di funzionalità. Quando la funzionalità è pronta per il rilascio, il ramo di funzionalità viene ricongiunto al ramo principale. Per ulteriori informazioni, consulta Informazioni sulle filiali (documentazione). GitHub

accesso break-glass

In circostanze eccezionali e tramite una procedura approvata, un mezzo rapido per consentire a un utente di accedere a un sito a Account AWS cui in genere non dispone delle autorizzazioni necessarie. Per ulteriori informazioni, vedere l'indicatore Implementate break-glass procedures nella guida Well-Architected AWS .

strategia brownfield

L'infrastruttura esistente nell'ambiente. Quando si adotta una strategia brownfield per un'architettura di sistema, si progetta l'architettura in base ai vincoli dei sistemi e dell'infrastruttura attuali. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

cache del buffer

L'area di memoria in cui sono archiviati i dati a cui si accede con maggiore frequenza.

capacità di business

Azioni intraprese da un'azienda per generare valore (ad esempio vendite, assistenza clienti o marketing). Le architetture dei microservizi e le decisioni di sviluppo possono essere guidate dalle capacità aziendali. Per ulteriori informazioni, consulta la sezione Organizzazione in base alle funzionalità aziendali del whitepaper Esecuzione di microservizi containerizzati su AWS.

pianificazione della continuità operativa (BCP)

Un piano che affronta il potenziale impatto di un evento che comporta l'interruzione dell'attività, come una migrazione su larga scala, sulle operazioni e consente a un'azienda di riprendere rapidamente le operazioni.

C

CAF

Vedi AWS Cloud Adoption Framework.

implementazione canaria

Il rilascio lento e incrementale di una versione agli utenti finali. Quando sei sicuro, distribuisci la nuova versione e sostituisci la versione corrente nella sua interezza.

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

Il processo di tracciamento delle modifiche a un'origine dati, ad esempio una tabella di database, e di registrazione dei metadati relativi alla modifica. È possibile utilizzare CDC per vari scopi, ad esempio il controllo o la replica delle modifiche in un sistema di destinazione per mantenere la sincronizzazione.

ingegneria del caos

Introduzione intenzionale di guasti o eventi dirompenti per testare la resilienza di un sistema. Puoi usare AWS Fault Injection Service (AWS FIS) per eseguire esperimenti che stressano i tuoi AWS carichi di lavoro e valutarne la risposta.

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

Un processo di categorizzazione che aiuta a generare previsioni. I modelli di ML per problemi di classificazione prevedono un valore discreto. I valori discreti sono sempre distinti l'uno dall'altro. Ad esempio, un modello potrebbe dover valutare se in un'immagine è presente o meno un'auto.

crittografia lato client

Crittografia dei dati a livello locale, prima che il destinatario li Servizio AWS riceva.

Centro di eccellenza cloud (CCoE)

Un team multidisciplinare che guida le iniziative di adozione del cloud in tutta l'organizzazione, tra cui lo sviluppo di best practice per il cloud, la mobilitazione delle risorse, la definizione delle tempistiche di migrazione e la guida dell'organizzazione attraverso trasformazioni su larga scala. Per ulteriori informazioni, consulta gli CCoE post sull' Cloud AWS Enterprise Strategy Blog.

cloud computing

La tecnologia cloud generalmente utilizzata per l'archiviazione remota di dati e la gestione dei dispositivi IoT. Il cloud computing è generalmente collegato alla tecnologia di edge computing.

modello operativo cloud

In un'organizzazione IT, il modello operativo utilizzato per creare, maturare e ottimizzare uno o più ambienti cloud. Per ulteriori informazioni, consulta Building your Cloud Operating Model.

fasi di adozione del cloud

Le quattro fasi che le organizzazioni in genere attraversano quando migrano verso Cloud AWS:

- Progetto: esecuzione di alcuni progetti relativi al cloud per scopi di dimostrazione e apprendimento
- Fondamento: effettuare investimenti fondamentali per scalare l'adozione del cloud (ad esempio, creazione di una landing zone, definizione di una CCo E, definizione di un modello operativo)
- Migrazione: migrazione di singole applicazioni
- Reinvenzione: ottimizzazione di prodotti e servizi e innovazione nel cloud

Queste fasi sono state definite da Stephen Orban nel post sul blog The Journey Toward Cloud-First & the Stages of Adoption on the Enterprise Strategy. Cloud AWS Per informazioni su come si relazionano alla strategia di AWS migrazione, consulta la guida alla preparazione alla migrazione.

CMDB

Vedi database di gestione della configurazione.

repository di codice

Una posizione in cui il codice di origine e altri asset, come documentazione, esempi e script, vengono archiviati e aggiornati attraverso processi di controllo delle versioni. Gli archivi cloud più comuni includono GitHub oBitbucket Cloud. Ogni versione del codice è denominata ramo. In una struttura a microservizi, ogni repository è dedicato a una singola funzionalità. Una singola pipeline CI/CD può utilizzare più repository.

cache fredda

Una cache del buffer vuota, non ben popolata o contenente dati obsoleti o irrilevanti. Ciò influisce sulle prestazioni perché l'istanza di database deve leggere dalla memoria o dal disco principale, il che richiede più tempo rispetto alla lettura dalla cache del buffer.

dati freddi

Dati a cui si accede raramente e che in genere sono storici. Quando si eseguono interrogazioni di questo tipo di dati, le interrogazioni lente sono in genere accettabili. Lo spostamento di questi dati su livelli o classi di storage meno costosi e con prestazioni inferiori può ridurre i costi.

visione artificiale (CV)

Un campo dell'intelligenza artificiale che utilizza l'apprendimento automatico per analizzare ed estrarre informazioni da formati visivi come immagini e video digitali. Ad esempio, Amazon SageMaker AI fornisce algoritmi di elaborazione delle immagini per CV.

deriva della configurazione

Per un carico di lavoro, una modifica della configurazione rispetto allo stato previsto. Potrebbe causare la non conformità del carico di lavoro e in genere è graduale e involontaria.

database di gestione della configurazione (CMDB)

Un repository che archivia e gestisce le informazioni su un database e il relativo ambiente IT, inclusi i componenti hardware e software e le relative configurazioni. In genere si utilizzano i dati di un CMDB nella fase di individuazione e analisi del portafoglio della migrazione.

Pacchetto di conformità

Una raccolta di AWS Config regole e azioni correttive che puoi assemblare per personalizzare i controlli di conformità e sicurezza. È possibile distribuire un pacchetto di conformità come singola entità in una regione Account AWS and o all'interno di un'organizzazione utilizzando un modello YAML. Per ulteriori informazioni, consulta i Conformance Pack nella documentazione. AWS Config

integrazione e distribuzione continua (continuous integration and continuous delivery, CI/CD)

Il processo di automazione delle fasi di origine, compilazione, test, gestione temporanea e produzione del processo di rilascio del software. CI/CD is commonly described as a pipeline. CI/CDpuò aiutarvi ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le consegne. Per ulteriori informazioni, consulta Vantaggi della distribuzione continua. CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta Distribuzione continua e implementazione continua a confronto.

CV

Vedi visione artificiale.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

Un processo per identificare e classificare i dati nella rete in base alla loro criticità e sensibilità. È un componente fondamentale di qualsiasi strategia di gestione dei rischi di sicurezza informatica perché consente di determinare i controlli di protezione e conservazione appropriati per i dati. La classificazione dei dati è un componente del pilastro della sicurezza nel AWS Well-Architected Framework. Per ulteriori informazioni, consulta Classificazione dei dati.

deriva dei dati

Una variazione significativa tra i dati di produzione e i dati utilizzati per addestrare un modello di machine learning o una modifica significativa dei dati di input nel tempo. La deriva dei dati può ridurre la qualità, l'accuratezza e l'equità complessive nelle previsioni dei modelli ML.

dati in transito

Dati che si spostano attivamente attraverso la rete, ad esempio tra le risorse di rete.

rete di dati

Un framework architettonico che fornisce la proprietà distribuita e decentralizzata dei dati con gestione e governance centralizzate.

riduzione al minimo dei dati

Il principio della raccolta e del trattamento dei soli dati strettamente necessari. Praticare la riduzione al minimo dei dati in the Cloud AWS può ridurre i rischi per la privacy, i costi e l'impronta di carbonio delle analisi.

perimetro dei dati

Una serie di barriere preventive nell' AWS ambiente che aiutano a garantire che solo le identità attendibili accedano alle risorse attendibili delle reti previste. Per ulteriori informazioni, consulta Building a data perimeter on. AWS

pre-elaborazione dei dati

Trasformare i dati grezzi in un formato che possa essere facilmente analizzato dal modello di ML. La pre-elaborazione dei dati può comportare la rimozione di determinate colonne o righe e l'eliminazione di valori mancanti, incoerenti o duplicati.

provenienza dei dati

Il processo di tracciamento dell'origine e della cronologia dei dati durante il loro ciclo di vita, ad esempio il modo in cui i dati sono stati generati, trasmessi e archiviati.

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

Un sistema di gestione dei dati che supporta la business intelligence, come l'analisi. I data warehouse contengono in genere grandi quantità di dati storici e vengono generalmente utilizzati per interrogazioni e analisi.

linguaggio di definizione del database (DDL)

Istruzioni o comandi per creare o modificare la struttura di tabelle e oggetti in un database.

linguaggio di manipolazione del database (DML)

Istruzioni o comandi per modificare (inserire, aggiornare ed eliminare) informazioni in un database.

DDL

Vedi linguaggio di definizione del database.

deep ensemble

Combinare più modelli di deep learning per la previsione. È possibile utilizzare i deep ensemble per ottenere una previsione più accurata o per stimare l'incertezza nelle previsioni.

deep learning

Un sottocampo del ML che utilizza più livelli di reti neurali artificiali per identificare la mappatura tra i dati di input e le variabili target di interesse.

defense-in-depth

Un approccio alla sicurezza delle informazioni in cui una serie di meccanismi e controlli di sicurezza sono accuratamente stratificati su una rete di computer per proteggere la riservatezza,

l'integrità e la disponibilità della rete e dei dati al suo interno. Quando si adotta questa strategia AWS, si aggiungono più controlli a diversi livelli della AWS Organizations struttura per proteggere le risorse. Ad esempio, un defense-in-depth approccio potrebbe combinare l'autenticazione a più fattori, la segmentazione della rete e la crittografia.

amministratore delegato

In AWS Organizations, un servizio compatibile può registrare un account AWS membro per amministrare gli account dell'organizzazione e gestire le autorizzazioni per quel servizio. Questo account è denominato amministratore delegato per quel servizio specifico. Per ulteriori informazioni e un elenco di servizi compatibili, consulta Servizi che funzionano con AWS Organizations nella documentazione di AWS Organizations .

implementazione

Il processo di creazione di un'applicazione, di nuove funzionalità o di correzioni di codice disponibili nell'ambiente di destinazione. L'implementazione prevede l'applicazione di modifiche in una base di codice, seguita dalla creazione e dall'esecuzione di tale base di codice negli ambienti applicativi.

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

Un controllo di sicurezza progettato per rilevare, registrare e avvisare dopo che si è verificato un evento. Questi controlli rappresentano una seconda linea di difesa e avvisano l'utente in caso di eventi di sicurezza che aggirano i controlli preventivi in vigore. Per ulteriori informazioni, consulta Controlli di rilevamento in Implementazione dei controlli di sicurezza in AWS.

mappatura del flusso di valore dello sviluppo (DVSM)

Un processo utilizzato per identificare e dare priorità ai vincoli che influiscono negativamente sulla velocità e sulla qualità nel ciclo di vita dello sviluppo del software. DVSM estende il processo di mappatura del flusso di valore originariamente progettato per pratiche di produzione snella. Si concentra sulle fasi e sui team necessari per creare e trasferire valore attraverso il processo di sviluppo del software.

gemello digitale

Una rappresentazione virtuale di un sistema reale, ad esempio un edificio, una fabbrica, un'attrezzatura industriale o una linea di produzione. I gemelli digitali supportano la manutenzione predittiva, il monitoraggio remoto e l'ottimizzazione della produzione.

tabella delle dimensioni

In uno schema a stella, una tabella più piccola che contiene gli attributi dei dati quantitativi in una tabella dei fatti. Gli attributi della tabella delle dimensioni sono in genere campi di testo o numeri discreti che si comportano come testo. Questi attributi vengono comunemente utilizzati per il vincolo delle query, il filtraggio e l'etichettatura dei set di risultati.

disastro

Un evento che impedisce a un carico di lavoro o a un sistema di raggiungere gli obiettivi aziendali nella sua sede principale di implementazione. Questi eventi possono essere disastri naturali, guasti tecnici o il risultato di azioni umane, come errori di configurazione involontari o attacchi di malware.

disaster recovery (DR)

La strategia e il processo utilizzati per ridurre al minimo i tempi di inattività e la perdita di dati causati da un disastro. Per ulteriori informazioni, consulta Disaster Recovery of Workloads su AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

Un approccio allo sviluppo di un sistema software complesso collegandone i componenti a domini in evoluzione, o obiettivi aziendali principali, perseguiti da ciascun componente. Questo concetto è stato introdotto da Eric Evans nel suo libro,Domain-Driven Design: Tackling Complexity in the Heart of Software (Boston: Addison-Wesley Professional, 2003). Per informazioni su come utilizzare la progettazione basata sul dominio con il modello del fico strangolatore (Strangler Fig), consulta la sezione Modernizzazione incrementale dei servizi Web Microsoft ASP.NET (ASMX) legacy utilizzando container e il Gateway Amazon API.

DOTT.

Vedi disaster recovery.

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, puoi utilizzarlo AWS CloudFormation per rilevare la deriva nelle risorse di sistema oppure puoi usarlo AWS Control Tower per rilevare cambiamenti nella tua landing zone che potrebbero influire sulla conformità ai requisiti di governance.

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

La tecnologia che aumenta la potenza di calcolo per i dispositivi intelligenti all'edge di una rete IoT. Rispetto al cloud computing, l'edge computing può ridurre la latenza di comunicazione e migliorare i tempi di risposta.

scambio elettronico di dati (EDI)

Lo scambio automatizzato di documenti aziendali tra organizzazioni. Per ulteriori informazioni, vedere Cos'è lo scambio elettronico di dati.

crittografia

Un processo di elaborazione che trasforma i dati in chiaro, leggibili dall'uomo, in testo cifrato.

chiave crittografica

Una stringa crittografica di bit randomizzati generata da un algoritmo di crittografia. Le chiavi possono variare di lunghezza e ogni chiave è progettata per essere imprevedibile e univoca.

endianità

L'ordine in cui i byte vengono archiviati nella memoria del computer. I sistemi big-endian memorizzano per primo il byte più importante. I sistemi little-endian memorizzano per primo il byte meno importante.

endpoint

Vedi service endpoint.

servizio endpoint

Un servizio che puoi ospitare in un cloud privato virtuale (VPC) da condividere con altri utenti. Puoi creare un servizio endpoint con AWS PrivateLink e concedere autorizzazioni ad altri Account AWS o a AWS Identity and Access Management (IAM) principali. Questi account o principali possono connettersi al servizio endpoint in privato creando endpoint VPC di interfaccia. Per ulteriori informazioni, consulta Creazione di un servizio endpoint nella documentazione di Amazon Virtual Private Cloud (Amazon VPC).

pianificazione delle risorse aziendali (ERP)

Un sistema che automatizza e gestisce i processi aziendali chiave (come contabilità, MES e gestione dei progetti) per un'azienda.

crittografia envelope

Il processo di crittografia di una chiave di crittografia con un'altra chiave di crittografia. Per ulteriori informazioni, vedete Envelope encryption nella documentazione AWS Key Management Service (AWS KMS).

ambiente

Un'istanza di un'applicazione in esecuzione. Di seguito sono riportati i tipi di ambiente più comuni nel cloud computing:

- ambiente di sviluppo: un'istanza di un'applicazione in esecuzione disponibile solo per il team principale responsabile della manutenzione dell'applicazione. Gli ambienti di sviluppo vengono utilizzati per testare le modifiche prima di promuoverle negli ambienti superiori. Questo tipo di ambiente viene talvolta definito ambiente di test.
- ambienti inferiori: tutti gli ambienti di sviluppo di un'applicazione, ad esempio quelli utilizzati per le build e i test iniziali.
- ambiente di produzione: un'istanza di un'applicazione in esecuzione a cui gli utenti finali possono accedere. In una pipeline CI/CD, l'ambiente di produzione è l'ultimo ambiente di implementazione.
- ambienti superiori: tutti gli ambienti a cui possono accedere utenti diversi dal team di sviluppo principale. Si può trattare di un ambiente di produzione, ambienti di preproduzione e ambienti per i test di accettazione da parte degli utenti.

epica

Nelle metodologie agili, categorie funzionali che aiutano a organizzare e dare priorità al lavoro. Le epiche forniscono una descrizione di alto livello dei requisiti e delle attività di implementazione.

Ad esempio, le epopee della sicurezza AWS CAF includono la gestione delle identità e degli accessi, i controlli investigativi, la sicurezza dell'infrastruttura, la protezione dei dati e la risposta agli incidenti. Per ulteriori informazioni sulle epiche, consulta la strategia di migrazione AWS , consulta la guida all'implementazione del programma.

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

Il processo di analisi di un set di dati per comprenderne le caratteristiche principali. Si raccolgono o si aggregano dati e quindi si eseguono indagini iniziali per trovare modelli, rilevare anomalie e verificare ipotesi. L'EDA viene eseguita calcolando statistiche di riepilogo e creando visualizzazioni di dati.

F

tabella dei fatti

Il tavolo centrale con schema a stella. Memorizza dati quantitativi sulle operazioni aziendali. In genere, una tabella dei fatti contiene due tipi di colonne: quelle che contengono misure e quelle che contengono una chiave esterna per una tabella di dimensioni.

fallire velocemente

Una filosofia che utilizza test frequenti e incrementali per ridurre il ciclo di vita dello sviluppo. È una parte fondamentale di un approccio agile.

limite di isolamento dei guasti

Nel Cloud AWS, un limite come una zona di disponibilità Regione AWS, un piano di controllo o un piano dati che limita l'effetto di un errore e aiuta a migliorare la resilienza dei carichi di lavoro. Per ulteriori informazioni, consulta AWS Fault Isolation Boundaries.

ramo di funzionalità

Vedi filiale.

caratteristiche

I dati di input che usi per fare una previsione. Ad esempio, in un contesto di produzione, le caratteristiche potrebbero essere immagini acquisite periodicamente dalla linea di produzione.

importanza delle caratteristiche

Quanto è importante una caratteristica per le previsioni di un modello. Di solito viene espresso come punteggio numerico che può essere calcolato con varie tecniche, come Shapley Additive Explanations (SHAP) e gradienti integrati. Per ulteriori informazioni, consulta Interpretabilità del modello di machine learning con AWS.

trasformazione delle funzionalità

Per ottimizzare i dati per il processo di machine learning, incluso l'arricchimento dei dati con fonti aggiuntive, il dimensionamento dei valori o l'estrazione di più set di informazioni da un singolo campo di dati. Ciò consente al modello di ML di trarre vantaggio dai dati. Ad esempio, se suddividi la data "2021-05-27 00:15:37" in "2021", "maggio", "giovedì" e "15", puoi aiutare l'algoritmo di apprendimento ad apprendere modelli sfumati associati a diversi componenti dei dati.

prompt con pochi scatti

Fornire a un LLM un numero limitato di esempi che dimostrino l'attività e il risultato desiderato prima di chiedergli di eseguire un'attività simile. Questa tecnica è un'applicazione dell'apprendimento contestuale, in cui i modelli imparano da esempi (immagini) incorporati nei prompt. I prompt con pochi passaggi possono essere efficaci per attività che richiedono una formattazione, un ragionamento o una conoscenza del dominio specifici. Vedi anche zero-shot prompting.

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

L'uso di più condizioni per consentire o rifiutare una richiesta di accesso.

migrazione flash-cut

Un metodo di migrazione del database che utilizza la replica continua dei dati tramite l'acquisizione dei dati delle modifiche per migrare i dati nel più breve tempo possibile, anziché utilizzare un approccio graduale. L'obiettivo è ridurre al minimo i tempi di inattività.

FM

Vedi il modello di base.

modello di fondazione (FM)

Una grande rete neurale di deep learning che si è addestrata su enormi set di dati generalizzati e non etichettati. FMs sono in grado di svolgere un'ampia varietà di attività generali, come

comprendere il linguaggio, generare testo e immagini e conversare in linguaggio naturale. Per ulteriori informazioni, consulta Cosa sono i modelli Foundation.

G

AI generativa

Un sottoinsieme di modelli di intelligenza artificiale che sono stati addestrati su grandi quantità di dati e che possono utilizzare un semplice prompt di testo per creare nuovi contenuti e artefatti, come immagini, video, testo e audio. Per ulteriori informazioni, consulta Cos'è l'IA generativa.

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

In Amazon CloudFront, un'opzione per impedire agli utenti di determinati paesi di accedere alle distribuzioni di contenuti. Puoi utilizzare un elenco consentito o un elenco di blocco per specificare i paesi approvati e vietati. Per ulteriori informazioni, consulta Limitare la distribuzione geografica dei contenuti nella CloudFront documentazione.

Flusso di lavoro di GitFlow

Un approccio in cui gli ambienti inferiori e superiori utilizzano rami diversi in un repository di codice di origine. Il flusso di lavoro Gitflow è considerato obsoleto e il flusso di lavoro basato su trunk è l'approccio moderno e preferito.

immagine dorata

Un'istantanea di un sistema o di un software che viene utilizzata come modello per distribuire nuove istanze di quel sistema o software. Ad esempio, nella produzione, un'immagine dorata può essere utilizzata per fornire software su più dispositivi e contribuire a migliorare la velocità, la scalabilità e la produttività nelle operazioni di produzione dei dispositivi.

strategia greenfield

L'assenza di infrastrutture esistenti in un nuovo ambiente. Quando si adotta una strategia greenfield per un'architettura di sistema, è possibile selezionare tutte le nuove tecnologie senza il vincolo della compatibilità con l'infrastruttura esistente, nota anche come brownfield. Per l'espansione dell'infrastruttura esistente, è possibile combinare strategie brownfield e greenfield.

guardrail

Una regola di alto livello che aiuta a governare le risorse, le politiche e la conformità tra le unità organizzative (). OUs I guardrail preventivi applicano le policy per garantire l'allineamento agli standard di conformità. Vengono implementati utilizzando le policy di controllo dei servizi e i limiti delle autorizzazioni IAM. I guardrail di rilevamento rilevano le violazioni delle policy e i problemi di conformità e generano avvisi per porvi rimedio. Sono implementati utilizzando Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector e controlli personalizzati AWS Lambda .

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

Migrazione del database di origine in un database di destinazione che utilizza un motore di database diverso (ad esempio, da Oracle ad Amazon Aurora). La migrazione eterogenea fa in genere parte di uno sforzo di riprogettazione e la conversione dello schema può essere un'attività complessa. AWS offre AWS SCT che aiuta con le conversioni dello schema.

alta disponibilità (HA)

La capacità di un carico di lavoro di funzionare in modo continuo, senza intervento, in caso di sfide o disastri. I sistemi HA sono progettati per il failover automatico, fornire costantemente prestazioni di alta qualità e gestire carichi e guasti diversi con un impatto minimo sulle prestazioni.

modernizzazione storica

Un approccio utilizzato per modernizzare e aggiornare i sistemi di tecnologia operativa (OT) per soddisfare meglio le esigenze dell'industria manifatturiera. Uno storico è un tipo di database utilizzato per raccogliere e archiviare dati da varie fonti in una fabbrica.

dati di esclusione

Una parte di dati storici etichettati che viene trattenuta da un set di dati utilizzata per addestrare un modello di apprendimento automatico. È possibile utilizzare i dati di holdout per valutare le prestazioni del modello confrontando le previsioni del modello con i dati di holdout.

migrazione di database omogenea

Migrazione del database di origine in un database di destinazione che condivide lo stesso motore di database (ad esempio, da Microsoft SQL Server ad Amazon RDS per SQL Server). La migrazione omogenea fa in genere parte di un'operazione di rehosting o ridefinizione della piattaforma. Per migrare lo schema è possibile utilizzare le utilità native del database.

dati caldi

Dati a cui si accede frequentemente, come dati in tempo reale o dati di traduzione recenti. Questi dati richiedono in genere un livello o una classe di storage ad alte prestazioni per fornire risposte rapide alle query.

hotfix

Una soluzione urgente per un problema critico in un ambiente di produzione. A causa della sua urgenza, un hotfix viene in genere creato al di fuori del tipico DevOps flusso di lavoro di rilascio.

periodo di hypercare

Subito dopo la conversione, il periodo di tempo in cui un team di migrazione gestisce e monitora le applicazioni migrate nel cloud per risolvere eventuali problemi. In genere, questo periodo dura da 1 a 4 giorni. Al termine del periodo di hypercare, il team addetto alla migrazione in genere trasferisce la responsabilità delle applicazioni al team addetto alle operazioni cloud.

I

IaC

Considera l'infrastruttura come codice.

Policy basata su identità

Una policy associata a uno o più principi IAM che definisce le relative autorizzazioni all'interno dell' Cloud AWS ambiente.

applicazione inattiva

Un'applicazione che prevede un uso di CPU e memoria medio compreso tra il 5% e il 20% in un periodo di 90 giorni. In un progetto di migrazione, è normale ritirare queste applicazioni o mantenerle on-premise.

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

Un modello che implementa una nuova infrastruttura per i carichi di lavoro di produzione anziché aggiornare, applicare patch o modificare l'infrastruttura esistente. Le infrastrutture immutabili sono intrinsecamente più coerenti, affidabili e prevedibili delle infrastrutture mutabili. Per ulteriori informazioni, consulta la best practice Deploy using immutable infrastructure in Well-Architected AWS Framework.

VPC in ingresso (ingress)

In un'architettura AWS multi-account, un VPC che accetta, ispeziona e indirizza le connessioni di rete dall'esterno di un'applicazione. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs per proteggere l'interfaccia bidirezionale tra l'applicazione e la rete Internet in generale.

migrazione incrementale

Una strategia di conversione in cui si esegue la migrazione dell'applicazione in piccole parti anziché eseguire una conversione singola e completa. Ad esempio, inizialmente potresti spostare solo alcuni microservizi o utenti nel nuovo sistema. Dopo aver verificato che tutto funzioni correttamente, puoi spostare in modo incrementale microservizi o utenti aggiuntivi fino alla disattivazione del sistema legacy. Questa strategia riduce i rischi associati alle migrazioni di grandi dimensioni.

Industria 4.0

Un termine introdotto da Klaus Schwab nel 2016 per riferirsi alla modernizzazione dei processi di produzione attraverso progressi in termini di connettività, dati in tempo reale, automazione, analisi e AI/ML.

infrastruttura

Tutte le risorse e gli asset contenuti nell'ambiente di un'applicazione.

infrastruttura come codice (IaC)

Il processo di provisioning e gestione dell'infrastruttura di un'applicazione tramite un insieme di file di configurazione. Il processo IaC è progettato per aiutarti a centralizzare la gestione dell'infrastruttura, a standardizzare le risorse e a dimensionare rapidamente, in modo che i nuovi ambienti siano ripetibili, affidabili e coerenti.

IIoInternet delle cose industriale (T)

L'uso di sensori e dispositivi connessi a Internet nei settori industriali, come quello manifatturiero, energetico, automobilistico, sanitario, delle scienze della vita e dell'agricoltura. Per ulteriori

informazioni, vedere Creazione di una strategia di trasformazione digitale per l'Internet of Things (IIoT) industriale.

VPC di ispezione

In un'architettura AWS multi-account, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPCs (nello stesso o in modo diverso Regioni AWS), Internet e le reti locali. La AWS Security Reference Architecture consiglia di configurare l'account di rete con informazioni in entrata, in uscita e di ispezione VPCs per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

Internet of Things (IoT)

La rete di oggetti fisici connessi con sensori o processori incorporati che comunicano con altri dispositivi e sistemi tramite Internet o una rete di comunicazione locale. Per ulteriori informazioni, consulta Cos'è l'IoT?

interpretabilità

Una caratteristica di un modello di machine learning che descrive il grado in cui un essere umano è in grado di comprendere in che modo le previsioni del modello dipendono dai suoi input. Per ulteriori informazioni, vedere Interpretabilità del modello di machine learning con. AWS

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

Una serie di best practice per offrire servizi IT e allinearli ai requisiti aziendali. ITIL fornisce le basi per ITSM.

gestione dei servizi IT (ITSM)

Attività associate alla progettazione, implementazione, gestione e supporto dei servizi IT per un'organizzazione. Per informazioni sull'integrazione delle operazioni cloud con gli strumenti ITSM, consulta la guida all'integrazione delle operazioni.

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

Un'implementazione del controllo di accesso obbligatorio (MAC) in cui agli utenti e ai dati stessi viene assegnato esplicitamente un valore di etichetta di sicurezza. L'intersezione tra l'etichetta di sicurezza utente e l'etichetta di sicurezza dei dati determina quali righe e colonne possono essere visualizzate dall'utente.

zona di destinazione

Una landing zone è un AWS ambiente multi-account ben progettato, scalabile e sicuro. Questo è un punto di partenza dal quale le organizzazioni possono avviare e distribuire rapidamente carichi di lavoro e applicazioni con fiducia nel loro ambiente di sicurezza e infrastruttura. Per ulteriori informazioni sulle zone di destinazione, consulta la sezione Configurazione di un ambiente AWS multi-account sicuro e scalabile.

modello linguistico di grandi dimensioni (LLM)

Un modello di intelligenza artificiale di deep learning preaddestrato su una grande quantità di dati. Un LLM può svolgere più attività, come rispondere a domande, riepilogare documenti, tradurre testo in altre lingue e completare frasi. Per ulteriori informazioni, consulta Cosa sono. LLMs

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

La best practice di sicurezza per la concessione delle autorizzazioni minime richieste per eseguire un'attività. Per ulteriori informazioni, consulta Applicazione delle autorizzazioni del privilegio minimo nella documentazione di IAM.

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

Un sistema che memorizza per primo il byte meno importante. Vedi anche endianità.

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

Un tipo di intelligenza artificiale che utilizza algoritmi e tecniche per il riconoscimento e l'apprendimento di schemi. Il machine learning analizza e apprende dai dati registrati, come i dati dell'Internet delle cose (IoT), per generare un modello statistico basato su modelli. Per ulteriori informazioni, consulta la sezione Machine learning.

ramo principale

Vedi filiale.

malware

Software progettato per compromettere la sicurezza o la privacy del computer. Il malware potrebbe interrompere i sistemi informatici, divulgare informazioni sensibili o ottenere accessi non autorizzati. Esempi di malware includono virus, worm, ransomware, trojan horse, spyware e keylogger.

servizi gestiti

Servizi AWS per cui AWS gestisce il livello di infrastruttura, il sistema operativo e le piattaforme e si accede agli endpoint per archiviare e recuperare i dati. Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3) e Amazon DynamoDB sono esempi di servizi gestiti. Questi sono noti anche come servizi astratti.

sistema di esecuzione della produzione (MES)

Un sistema software per tracciare, monitorare, documentare e controllare i processi di produzione che convertono le materie prime in prodotti finiti in officina.

MAP

Vedi Migration Acceleration Program.

meccanismo

Un processo completo in cui si crea uno strumento, si promuove l'adozione dello strumento e quindi si esaminano i risultati per apportare le modifiche. Un meccanismo è un ciclo che si rafforza e si migliora man mano che funziona. Per ulteriori informazioni, consulta Creazione di meccanismi nel AWS Well-Architected Framework.

account membro

Tutti gli account Account AWS diversi dall'account di gestione che fanno parte di un'organizzazione in. AWS Organizations Un account può essere membro di una sola organizzazione alla volta.

MEH.

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

Un protocollo di comunicazione machine-to-machine (M2M) leggero, basato sul modello di pubblicazione/sottoscrizione, per dispositivi IoT con risorse limitate.

microservizio

Un servizio piccolo e indipendente che comunica tramite canali ben definiti ed è in genere di proprietà di piccoli team autonomi. APIs Ad esempio, un sistema assicurativo potrebbe includere microservizi che si riferiscono a funzionalità aziendali, come vendite o marketing, o sottodomini, come acquisti, reclami o analisi. I vantaggi dei microservizi includono agilità, dimensionamento flessibile, facilità di implementazione, codice riutilizzabile e resilienza. Per ulteriori informazioni, consulta Integrazione dei microservizi utilizzando servizi serverless. AWS

architettura di microservizi

Un approccio alla creazione di un'applicazione con componenti indipendenti che eseguono ogni processo applicativo come microservizio. Questi microservizi comunicano attraverso un'interfaccia ben definita utilizzando sistemi leggeri. APIs Ogni microservizio in questa architettura può essere aggiornato, distribuito e dimensionato per soddisfare la richiesta di funzioni specifiche di un'applicazione. Per ulteriori informazioni, vedere Implementazione dei microservizi su. AWS

Programma di accelerazione della migrazione (MAP)

Un AWS programma che fornisce consulenza, supporto, formazione e servizi per aiutare le organizzazioni a costruire una solida base operativa per il passaggio al cloud e per contribuire a compensare il costo iniziale delle migrazioni. MAP include una metodologia di migrazione per

eseguire le migrazioni precedenti in modo metodico e un set di strumenti per automatizzare e accelerare gli scenari di migrazione comuni.

migrazione su larga scala

Il processo di trasferimento della maggior parte del portfolio di applicazioni sul cloud avviene a ondate, con più applicazioni trasferite a una velocità maggiore in ogni ondata. Questa fase utilizza le migliori pratiche e le lezioni apprese nelle fasi precedenti per implementare una fabbrica di migrazione di team, strumenti e processi per semplificare la migrazione dei carichi di lavoro attraverso l'automazione e la distribuzione agile. Questa è la terza fase della strategia di migrazione AWS.

fabbrica di migrazione

Team interfunzionali che semplificano la migrazione dei carichi di lavoro attraverso approcci automatizzati e agili. I team di Migration Factory in genere includono addetti alle operazioni, analisti e proprietari aziendali, ingegneri addetti alla migrazione, sviluppatori e DevOps professionisti che lavorano nell'ambito degli sprint. Tra il 20% e il 50% di un portfolio di applicazioni aziendali è costituito da schemi ripetuti che possono essere ottimizzati con un approccio di fabbrica. Per ulteriori informazioni, consulta la discussione sulle fabbriche di migrazione e la Guida alla fabbrica di migrazione al cloud in questo set di contenuti.

metadati di migrazione

Le informazioni sull'applicazione e sul server necessarie per completare la migrazione. Ogni modello di migrazione richiede un set diverso di metadati di migrazione. Esempi di metadati di migrazione includono la sottorete, il gruppo di sicurezza e l'account di destinazione. AWS

modello di migrazione

Un'attività di migrazione ripetibile che descrive in dettaglio la strategia di migrazione, la destinazione della migrazione e l'applicazione o il servizio di migrazione utilizzati. Esempio: riorganizza la migrazione su Amazon EC2 con AWS Application Migration Service.

Valutazione del portfolio di migrazione (MPA)

Uno strumento online che fornisce informazioni per la convalida del business case per la migrazione a. Cloud AWS MPA offre una valutazione dettagliata del portfolio (dimensionamento corretto dei server, prezzi, confronto del TCO, analisi dei costi di migrazione) e pianificazione della migrazione (analisi e raccolta dei dati delle applicazioni, raggruppamento delle applicazioni, prioritizzazione delle migrazioni e pianificazione delle ondate). Lo strumento MPA (richiede l'accesso) è disponibile gratuitamente per tutti i AWS consulenti e i consulenti dei partner APN.

valutazione della preparazione alla migrazione (MRA)

Il processo di acquisizione di informazioni sullo stato di preparazione al cloud di un'organizzazione, l'identificazione dei punti di forza e di debolezza e la creazione di un piano d'azione per colmare le lacune identificate, utilizzando il CAF. AWS Per ulteriori informazioni, consulta la guida di preparazione alla migrazione. MRA è la prima fase della strategia di migrazione AWS.

strategia di migrazione

L'approccio utilizzato per migrare un carico di lavoro verso. Cloud AWS Per ulteriori informazioni, consulta la voce 7 R in questo glossario e consulta Mobilita la tua organizzazione per accelerare le migrazioni su larga scala.

ML

Vedi machine learning.

modernizzazione

Trasformazione di un'applicazione obsoleta (legacy o monolitica) e della relativa infrastruttura in un sistema agile, elastico e altamente disponibile nel cloud per ridurre i costi, aumentare l'efficienza e sfruttare le innovazioni. Per ulteriori informazioni, vedere Strategia per la modernizzazione delle applicazioni in. Cloud AWS

valutazione della preparazione alla modernizzazione

Una valutazione che aiuta a determinare la preparazione alla modernizzazione delle applicazioni di un'organizzazione, identifica vantaggi, rischi e dipendenze e determina in che misura l'organizzazione può supportare lo stato futuro di tali applicazioni. Il risultato della valutazione è uno schema dell'architettura di destinazione, una tabella di marcia che descrive in dettaglio le fasi di sviluppo e le tappe fondamentali del processo di modernizzazione e un piano d'azione per colmare le lacune identificate. Per ulteriori informazioni, vedere Valutazione della preparazione alla modernizzazione per le applicazioni in. Cloud AWS

applicazioni monolitiche (monoliti)

Applicazioni eseguite come un unico servizio con processi strettamente collegati. Le applicazioni monolitiche presentano diversi inconvenienti. Se una funzionalità dell'applicazione registra un picco di domanda, l'intera architettura deve essere dimensionata. L'aggiunta o il miglioramento delle funzionalità di un'applicazione monolitica diventa inoltre più complessa man mano che la base di codice cresce. Per risolvere questi problemi, puoi utilizzare un'architettura di microservizi. Per ulteriori informazioni, consulta la sezione Scomposizione dei monoliti in microservizi.

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

Un processo che aiuta a generare previsioni per più classi (prevedendo uno o più di due risultati). Ad esempio, un modello di machine learning potrebbe chiedere "Questo prodotto è un libro, un'auto o un telefono?" oppure "Quale categoria di prodotti è più interessante per questo cliente?"

infrastruttura mutabile

Un modello che aggiorna e modifica l'infrastruttura esistente per i carichi di lavoro di produzione. Per migliorare la coerenza, l'affidabilità e la prevedibilità, il AWS Well-Architected Framework consiglia l'uso di un'infrastruttura immutabile come best practice.

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

Un metodo di migrazione in cui il carico di lavoro di origine viene eliminato durante il processo di migrazione. Questo metodo prevede tempi di inattività prolungati e viene in genere utilizzato per carichi di lavoro piccoli e non critici.

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

Un metodo di migrazione in cui il carico di lavoro di origine viene copiato sul sistema di destinazione senza essere messo offline. Le applicazioni connesse al carico di lavoro possono continuare a funzionare durante la migrazione. Questo metodo comporta tempi di inattività pari a zero o comunque minimi e viene in genere utilizzato per carichi di lavoro di produzione critici.

OPC-UA

Vedi Open Process Communications - Unified Architecture.

Comunicazioni a processo aperto - Architettura unificata (OPC-UA)

Un protocollo di comunicazione machine-to-machine (M2M) per l'automazione industriale. OPC-UA fornisce uno standard di interoperabilità con schemi di crittografia, autenticazione e autorizzazione dei dati.

accordo a livello operativo (OLA)

Un accordo che chiarisce quali sono gli impegni reciproci tra i gruppi IT funzionali, a supporto di un accordo sul livello di servizio (SLA).

revisione della prontezza operativa (ORR)

Un elenco di domande e best practice associate che aiutano a comprendere, valutare, prevenire o ridurre la portata degli incidenti e dei possibili guasti. Per ulteriori informazioni, vedere Operational Readiness Reviews (ORR) nel Well-Architected AWS Framework.

tecnologia operativa (OT)

Sistemi hardware e software che interagiscono con l'ambiente fisico per controllare le operazioni, le apparecchiature e le infrastrutture industriali. Nella produzione, l'integrazione di sistemi OT e di tecnologia dell'informazione (IT) è un obiettivo chiave per le trasformazioni dell'Industria 4.0.

integrazione delle operazioni (OI)

Il processo di modernizzazione delle operazioni nel cloud, che prevede la pianificazione, l'automazione e l'integrazione della disponibilità. Per ulteriori informazioni, consulta la guida all'integrazione delle operazioni.

trail organizzativo

Un percorso creato da noi AWS CloudTrail che registra tutti gli eventi di un'organizzazione per tutti Account AWS . AWS Organizations Questo percorso viene creato in ogni Account AWS che

fa parte dell'organizzazione e tiene traccia dell'attività in ogni account. Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione nella CloudTrail documentazione.

gestione del cambiamento organizzativo (OCM)

Un framework per la gestione di trasformazioni aziendali importanti e che comportano l'interruzione delle attività dal punto di vista delle persone, della cultura e della leadership. OCM aiuta le organizzazioni a prepararsi e passare a nuovi sistemi e strategie accelerando l'adozione del cambiamento, affrontando i problemi di transizione e promuovendo cambiamenti culturali e organizzativi. Nella strategia di AWS migrazione, questo framework si chiama accelerazione delle persone, a causa della velocità di cambiamento richiesta nei progetti di adozione del cloud. Per ulteriori informazioni, consultare la Guida OCM.

controllo dell'accesso all'origine (OAC)

In CloudFront, un'opzione avanzata per limitare l'accesso per proteggere i contenuti di Amazon Simple Storage Service (Amazon S3). OAC supporta tutti i bucket S3 in generale Regioni AWS, la crittografia lato server con AWS KMS (SSE-KMS) e le richieste dinamiche e dirette al bucket S3. `PUT DELETE`

identità di accesso origine (OAI)

Nel CloudFront, un'opzione per limitare l'accesso per proteggere i tuoi contenuti Amazon S3. Quando usi OAI, CloudFront crea un principale con cui Amazon S3 può autenticarsi. I principali autenticati possono accedere ai contenuti in un bucket S3 solo tramite una distribuzione specifica. CloudFront Vedi anche OAC, che fornisce un controllo degli accessi più granulare e avanzato.

ORR

Vedi la revisione della prontezza operativa.

- NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

In un'architettura AWS multi-account, un VPC che gestisce le connessioni di rete avviate dall'interno di un'applicazione. La AWS Security Reference Architecture consiglia di configurare l'account di rete con funzionalità in entrata, in uscita e di ispezione VPCs per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

P

limite delle autorizzazioni

Una policy di gestione IAM collegata ai principali IAM per impostare le autorizzazioni massime che l'utente o il ruolo possono avere. Per ulteriori informazioni, consulta Limiti delle autorizzazioni nella documentazione di IAM.

informazioni di identificazione personale (PII)

Informazioni che, se visualizzate direttamente o abbinate ad altri dati correlati, possono essere utilizzate per dedurre ragionevolmente l'identità di un individuo. Esempi di informazioni personali includono nomi, indirizzi e informazioni di contatto.

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

Una serie di passaggi predefiniti che raccolgono il lavoro associato alle migrazioni, come l'erogazione delle funzioni operative principali nel cloud. Un playbook può assumere la forma di script, runbook automatici o un riepilogo dei processi o dei passaggi necessari per gestire un ambiente modernizzato.

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

Un oggetto in grado di definire le autorizzazioni (vedi politica basata sull'identità), specificare le condizioni di accesso (vedi politicabasata sulle risorse) o definire le autorizzazioni massime per tutti gli account di un'organizzazione in (vedi politica di controllo dei servizi). AWS Organizations

persistenza poliglotta

Scelta indipendente della tecnologia di archiviazione di dati di un microservizio in base ai modelli di accesso ai dati e ad altri requisiti. Se i microservizi utilizzano la stessa tecnologia di archiviazione di dati, possono incontrare problemi di implementazione o registrare prestazioni

scadenti. I microservizi vengono implementati più facilmente e ottengono prestazioni e scalabilità migliori se utilizzano l'archivio dati più adatto alle loro esigenze. Per ulteriori informazioni, consulta la sezione Abilitazione della persistenza dei dati nei microservizi.

valutazione del portfolio

Un processo di scoperta, analisi e definizione delle priorità del portfolio di applicazioni per pianificare la migrazione. Per ulteriori informazioni, consulta la pagina Valutazione della preparazione alla migrazione.

predicate

Una condizione di interrogazione che restituisce o, in genere, si trova in una clausola`WHERE`. `true` `false`

predicato pushdown

Una tecnica di ottimizzazione delle query del database che filtra i dati della query prima del trasferimento. Ciò riduce la quantità di dati che devono essere recuperati ed elaborati dal database relazionale e migliora le prestazioni delle query.

controllo preventivo

Un controllo di sicurezza progettato per impedire il verificarsi di un evento. Questi controlli sono la prima linea di difesa per impedire accessi non autorizzati o modifiche indesiderate alla rete. Per ulteriori informazioni, consulta Controlli preventivi in Implementazione dei controlli di sicurezza in AWS.

principale

Un'entità in AWS grado di eseguire azioni e accedere alle risorse. Questa entità è in genere un utente root per un Account AWS ruolo IAM o un utente. Per ulteriori informazioni, consulta Principali in Termini e concetti dei ruoli nella documentazione di IAM.

privacy fin dalla progettazione

Un approccio di ingegneria dei sistemi che tiene conto della privacy durante l'intero processo di sviluppo.

zone ospitate private

Un contenitore che contiene informazioni su come desideri che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più. VPCs Per ulteriori informazioni, consulta Utilizzo delle zone ospitate private nella documentazione di Route 53.

controllo proattivo

Un controllo di sicurezza progettato per impedire l'implementazione di risorse non conformi. Questi controlli analizzano le risorse prima del loro provisioning. Se la risorsa non è conforme al controllo, non viene fornita. Per ulteriori informazioni, consulta la guida di riferimento sui controlli nella AWS Control Tower documentazione e consulta Controlli proattivi in Implementazione dei controlli di sicurezza su. AWS

gestione del ciclo di vita del prodotto (PLM)

La gestione dei dati e dei processi di un prodotto durante l'intero ciclo di vita, dalla progettazione, sviluppo e lancio, attraverso la crescita e la maturità, fino al declino e alla rimozione.

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

Nella produzione, un computer altamente affidabile e adattabile che monitora le macchine e automatizza i processi di produzione.

concatenamento rapido

Utilizzo dell'output di un prompt LLM come input per il prompt successivo per generare risposte migliori. Questa tecnica viene utilizzata per suddividere un'attività complessa in sottoattività o per perfezionare o espandere iterativamente una risposta preliminare. Aiuta a migliorare l'accuratezza e la pertinenza delle risposte di un modello e consente risultati più granulari e personalizzati.

pseudonimizzazione

Il processo di sostituzione degli identificatori personali in un set di dati con valori segnaposto. La pseudonimizzazione può aiutare a proteggere la privacy personale. I dati pseudonimizzati sono ancora considerati dati personali.

publish/subscribe (pub/sub)

Un modello che consente comunicazioni asincrone tra microservizi per migliorare la scalabilità e la reattività. Ad esempio, in un MES basato su microservizi, un microservizio può pubblicare messaggi di eventi su un canale a cui altri microservizi possono abbonarsi. Il sistema può aggiungere nuovi microservizi senza modificare il servizio di pubblicazione.

Q

Piano di query

Una serie di passaggi, come le istruzioni, utilizzati per accedere ai dati in un sistema di database relazionale SQL.

regressione del piano di query

Quando un ottimizzatore del servizio di database sceglie un piano non ottimale rispetto a prima di una determinata modifica all'ambiente di database. Questo può essere causato da modifiche a statistiche, vincoli, impostazioni dell'ambiente, associazioni dei parametri di query e aggiornamenti al motore di database.

R

Matrice RACI

Vedi responsabile, responsabile, consultato, informato (RACI).

STRACCIO

Vedi Retrieval Augmented Generation.

ransomware

Un software dannoso progettato per bloccare l'accesso a un sistema informatico o ai dati fino a quando non viene effettuato un pagamento.

Matrice RASCI

Vedi responsabile, responsabile, consultato, informato (RACI).

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

Una copia di un database utilizzata per scopi di sola lettura. È possibile indirizzare le query alla replica di lettura per ridurre il carico sul database principale.

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

Il periodo di tempo massimo accettabile dall'ultimo punto di ripristino dei dati. Questo determina ciò che si considera una perdita di dati accettabile tra l'ultimo punto di ripristino e l'interruzione del servizio.

obiettivo del tempo di ripristino (RTO)

Il ritardo massimo accettabile tra l'interruzione del servizio e il ripristino del servizio.

rifattorizzare

Vedi 7 R.

Regione

Una raccolta di AWS risorse in un'area geografica. Ciascuna Regione AWS è isolata e indipendente dalle altre per fornire tolleranza agli errori, stabilità e resilienza. Per ulteriori informazioni, consulta Specificare cosa può usare Regioni AWS il tuo account.

regressione

Una tecnica di ML che prevede un valore numerico. Ad esempio, per risolvere il problema "A che prezzo verrà venduta questa casa?" un modello di ML potrebbe utilizzare un modello di regressione lineare per prevedere il prezzo di vendita di una casa sulla base di dati noti sulla casa (ad esempio, la metratura).

riospitare

Vedi 7 R.

rilascio

In un processo di implementazione, l'atto di promuovere modifiche a un ambiente di produzione.

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

La capacità di un'applicazione di resistere o ripristinare le interruzioni. L'elevata disponibilità e il disaster recovery sono considerazioni comuni quando si pianifica la resilienza in. Cloud AWSPer ulteriori informazioni, vedere Cloud AWS Resilience.

policy basata su risorse

Una policy associata a una risorsa, ad esempio un bucket Amazon S3, un endpoint o una chiave di crittografia. Questo tipo di policy specifica a quali principali è consentito l'accesso, le azioni supportate e qualsiasi altra condizione che deve essere soddisfatta.

matrice di assegnazione di responsabilità (RACI)

Una matrice che definisce i ruoli e le responsabilità di tutte le parti coinvolte nelle attività di migrazione e nelle operazioni cloud. Il nome della matrice deriva dai tipi di responsabilità definiti nella matrice: responsabile (R), responsabile (A), consultato (C) e informato (I). Il tipo di supporto (S) è facoltativo. Se includi il supporto, la matrice viene chiamata matrice RASCI e, se la escludi, viene chiamata matrice RACI.

controllo reattivo

Un controllo di sicurezza progettato per favorire la correzione di eventi avversi o deviazioni dalla baseline di sicurezza. Per ulteriori informazioni, consulta Controlli reattivi in Implementazione dei controlli di sicurezza in AWS.

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

Una tecnologia di intelligenza artificiale generativa in cui un LLM fa riferimento a una fonte di dati autorevole esterna alle sue fonti di dati di formazione prima di generare una risposta. Ad esempio, un modello RAG potrebbe eseguire una ricerca semantica nella knowledge base o nei dati personalizzati di un'organizzazione. Per ulteriori informazioni, consulta Cos'è il RAG.

rotazione

Processo di aggiornamento periodico di un segreto per rendere più difficile l'accesso alle credenziali da parte di un utente malintenzionato.

controllo dell'accesso a righe e colonne (RCAC)

L'uso di espressioni SQL di base e flessibili con regole di accesso definite. RCAC è costituito da autorizzazioni di riga e maschere di colonna.

RPO

Vedi l'obiettivo del punto di ripristino.

RTO

Vedi l'obiettivo del tempo di ripristino.

runbook

Un insieme di procedure manuali o automatizzate necessarie per eseguire un'attività specifica. In genere sono progettati per semplificare operazioni o procedure ripetitive con tassi di errore elevati.

S

SAML 2.0

Uno standard aperto utilizzato da molti provider di identità (IdPs). Questa funzionalità abilita il single sign-on (SSO) federato, in modo che gli utenti possano accedere AWS Management Console o chiamare le operazioni AWS API senza che tu debba creare un utente in IAM per tutti i membri dell'organizzazione. Per ulteriori informazioni sulla federazione basata su SAML 2.0, consulta Informazioni sulla federazione basata su SAML 2.0 nella documentazione di IAM.

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

In AWS Secrets Manager, informazioni riservate o riservate, come una password o le credenziali utente, archiviate in forma crittografata. È costituito dal valore segreto e dai relativi metadati. Il valore segreto può essere binario, una stringa singola o più stringhe. Per ulteriori informazioni, consulta Cosa c'è in un segreto di Secrets Manager? nella documentazione di Secrets Manager.

sicurezza fin dalla progettazione

Un approccio di ingegneria dei sistemi che tiene conto della sicurezza durante l'intero processo di sviluppo.

controllo di sicurezza

Un guardrail tecnico o amministrativo che impedisce, rileva o riduce la capacità di un autore di minacce di sfruttare una vulnerabilità di sicurezza. Esistono quattro tipi principali di controlli di sicurezza: preventivi, investigativi, reattivi e proattivi.

rafforzamento della sicurezza

Il processo di riduzione della superficie di attacco per renderla più resistente agli attacchi. Può includere azioni come la rimozione di risorse che non sono più necessarie, l'implementazione di best practice di sicurezza che prevedono la concessione del privilegio minimo o la disattivazione di funzionalità non necessarie nei file di configurazione.

sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM)

Strumenti e servizi che combinano sistemi di gestione delle informazioni di sicurezza (SIM) e sistemi di gestione degli eventi di sicurezza (SEM). Un sistema SIEM raccoglie, monitora e analizza i dati da server, reti, dispositivi e altre fonti per rilevare minacce e violazioni della sicurezza e generare avvisi.

automazione della risposta alla sicurezza

Un'azione predefinita e programmata progettata per rispondere o porre rimedio automaticamente a un evento di sicurezza. Queste automazioni fungono da controlli di sicurezza investigativi o reattivi che aiutano a implementare le migliori pratiche di sicurezza. AWS Esempi di azioni di risposta automatizzate includono la modifica di un gruppo di sicurezza VPC, l'applicazione di patch a un'istanza EC2 Amazon o la rotazione delle credenziali.

Crittografia lato server

Crittografia dei dati a destinazione, da parte di chi li riceve. Servizio AWS

Policy di controllo dei servizi (SCP)

Una politica che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in. AWS Organizations SCPs definire barriere o fissare limiti alle azioni che un amministratore può delegare a utenti o ruoli. È possibile utilizzarli SCPs come elenchi consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per

ulteriori informazioni, consulta le politiche di controllo del servizio nella AWS Organizations documentazione.

endpoint del servizio

L'URL del punto di ingresso per un Servizio AWS. Puoi utilizzare l'endpoint per connetterti a livello di programmazione al servizio di destinazione. Per ulteriori informazioni, consulta Endpoint del Servizio AWS nei Riferimenti generali di AWS.

accordo sul livello di servizio (SLA)

Un accordo che chiarisce ciò che un team IT promette di offrire ai propri clienti, ad esempio l'operatività e le prestazioni del servizio.

indicatore del livello di servizio (SLI)

Misurazione di un aspetto prestazionale di un servizio, ad esempio il tasso di errore, la disponibilità o la velocità effettiva.

obiettivo a livello di servizio (SLO)

Una metrica target che rappresenta lo stato di un servizio, misurato da un indicatore del livello di servizio.

Modello di responsabilità condivisa

Un modello che descrive la responsabilità condivisa AWS per la sicurezza e la conformità del cloud. AWS è responsabile della sicurezza del cloud, mentre tu sei responsabile della sicurezza nel cloud. Per ulteriori informazioni, consulta Modello di responsabilità condivisa.

SIEM

Vedi il sistema di gestione delle informazioni e degli eventi sulla sicurezza.

punto di errore singolo (SPOF)

Un guasto in un singolo componente critico di un'applicazione che può disturbare il sistema.

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

Un modello per dimensionare e accelerare i progetti di modernizzazione. Man mano che vengono definite nuove funzionalità e versioni dei prodotti, il team principale si divide per creare nuovi team di prodotto. Questo aiuta a dimensionare le capacità e i servizi dell'organizzazione, migliora la produttività degli sviluppatori e supporta una rapida innovazione. Per ulteriori informazioni, vedere Approccio graduale alla modernizzazione delle applicazioni in. Cloud AWS

SPOF

Vedi punto di errore singolo.

schema a stella

Una struttura organizzativa di database che utilizza un'unica tabella dei fatti di grandi dimensioni per archiviare i dati transazionali o misurati e utilizza una o più tabelle dimensionali più piccole per memorizzare gli attributi dei dati. Questa struttura è progettata per l'uso in un data warehouse o per scopi di business intelligence.

modello del fico strangolatore

Un approccio alla modernizzazione dei sistemi monolitici mediante la riscrittura e la sostituzione incrementali delle funzionalità del sistema fino alla disattivazione del sistema legacy. Questo modello utilizza l'analogia di una pianta di fico che cresce fino a diventare un albero robusto e alla fine annienta e sostituisce il suo ospite. Il modello è stato introdotto da Martin Fowler come metodo per gestire il rischio durante la riscrittura di sistemi monolitici. Per un esempio di come applicare questo modello, consulta Modernizzazione incrementale dei servizi Web legacy di Microsoft ASP.NET (ASMX) mediante container e Gateway Amazon API.

sottorete

Un intervallo di indirizzi IP nel VPC. Una sottorete deve risiedere in una singola zona di disponibilità.

controllo di supervisione e acquisizione dati (SCADA)

Nella produzione, un sistema che utilizza hardware e software per monitorare gli asset fisici e le operazioni di produzione.

crittografia simmetrica

Un algoritmo di crittografia che utilizza la stessa chiave per crittografare e decrittografare i dati.

test sintetici

Test di un sistema in modo da simulare le interazioni degli utenti per rilevare potenziali problemi o monitorare le prestazioni. Puoi usare Amazon CloudWatch Synthetics per creare questi test.

prompt di sistema

Una tecnica per fornire contesto, istruzioni o linee guida a un LLM per indirizzarne il comportamento. I prompt di sistema aiutano a impostare il contesto e stabilire regole per le interazioni con gli utenti.

T

tags

Coppie chiave-valore che fungono da metadati per l'organizzazione delle risorse. AWS Con i tag è possibile a gestire, identificare, organizzare, cercare e filtrare le risorse. Per ulteriori informazioni, consulta Tagging delle risorse AWS.

variabile di destinazione

Il valore che stai cercando di prevedere nel machine learning supervisionato. Questo è indicato anche come variabile di risultato. Ad esempio, in un ambiente di produzione la variabile di destinazione potrebbe essere un difetto del prodotto.

elenco di attività

Uno strumento che viene utilizzato per tenere traccia dei progressi tramite un runbook. Un elenco di attività contiene una panoramica del runbook e un elenco di attività generali da completare. Per ogni attività generale, include la quantità stimata di tempo richiesta, il proprietario e lo stato di avanzamento.

Ambiente di test

Vedi ambiente.

training

Fornire dati da cui trarre ispirazione dal modello di machine learning. I dati di training devono contenere la risposta corretta. L'algoritmo di apprendimento trova nei dati di addestramento i pattern che mappano gli attributi dei dati di input al target (la risposta che si desidera prevedere). Produce un modello di ML che acquisisce questi modelli. Puoi quindi utilizzare il modello di ML per creare previsioni su nuovi dati di cui non si conosce il target.

Transit Gateway

Un hub di transito di rete che puoi utilizzare per interconnettere le tue reti VPCs e quelle locali. Per ulteriori informazioni, consulta Cos'è un gateway di transito nella AWS Transit Gateway documentazione.

flusso di lavoro basato su trunk

Un approccio in cui gli sviluppatori creano e testano le funzionalità localmente in un ramo di funzionalità e quindi uniscono tali modifiche al ramo principale. Il ramo principale viene quindi integrato negli ambienti di sviluppo, preproduzione e produzione, in sequenza.

Accesso attendibile

Concessione delle autorizzazioni a un servizio specificato dall'utente per eseguire attività all'interno dell'organizzazione AWS Organizations e nei suoi account per conto dell'utente. Il servizio attendibile crea un ruolo collegato al servizio in ogni account, quando tale ruolo è necessario, per eseguire attività di gestione per conto dell'utente. Per ulteriori informazioni, consulta Utilizzo AWS Organizations con altri AWS servizi nella AWS Organizations documentazione.

regolazione

Modificare alcuni aspetti del processo di training per migliorare la precisione del modello di ML. Ad esempio, puoi addestrare il modello di ML generando un set di etichette, aggiungendo etichette e quindi ripetendo questi passaggi più volte con impostazioni diverse per ottimizzare il modello.

team da due pizze

Una piccola DevOps squadra che puoi sfamare con due pizze. Un team composto da due persone garantisce la migliore opportunità possibile di collaborazione nello sviluppo del software.

U

incertezza

Un concetto che si riferisce a informazioni imprecise, incomplete o sconosciute che possono minare l'affidabilità dei modelli di machine learning predittivi. Esistono due tipi di incertezza: l'incertezza epistemica, che è causata da dati limitati e incompleti, mentre l'incertezza aleatoria è causata dal rumore e dalla casualità insiti nei dati. Per ulteriori informazioni, consulta la guida Quantificazione dell'incertezza nei sistemi di deep learning.

compiti indifferenziati

Conosciuto anche come sollevamento di carichi pesanti, è un lavoro necessario per creare e far funzionare un'applicazione, ma che non apporta valore diretto all'utente finale né offre vantaggi competitivi. Esempi di attività indifferenziate includono l'approvvigionamento, la manutenzione e la pianificazione della capacità.

ambienti superiori

Vedi ambiente.

V

vacuum

Un'operazione di manutenzione del database che prevede la pulizia dopo aggiornamenti incrementali per recuperare lo spazio di archiviazione e migliorare le prestazioni.

controllo delle versioni

Processi e strumenti che tengono traccia delle modifiche, ad esempio le modifiche al codice di origine in un repository.

Peering VPC

Una connessione tra due VPCs che consente di indirizzare il traffico utilizzando indirizzi IP privati. Per ulteriori informazioni, consulta Che cos'è il peering VPC? nella documentazione di Amazon VPC.

vulnerabilità

Un difetto software o hardware che compromette la sicurezza del sistema.

W

cache calda

Una cache del buffer che contiene dati correnti e pertinenti a cui si accede frequentemente. L'istanza di database può leggere dalla cache del buffer, il che richiede meno tempo rispetto alla lettura dalla memoria dal disco principale.

dati caldi

Dati a cui si accede raramente. Quando si eseguono interrogazioni di questo tipo di dati, in genere sono accettabili query moderatamente lente.

funzione finestra

Una funzione SQL che esegue un calcolo su un gruppo di righe che si riferiscono in qualche modo al record corrente. Le funzioni della finestra sono utili per l'elaborazione di attività, come il calcolo di una media mobile o l'accesso al valore delle righe in base alla posizione relativa della riga corrente.

Carico di lavoro

Una raccolta di risorse e codice che fornisce valore aziendale, ad esempio un'applicazione rivolta ai clienti o un processo back-end.

flusso di lavoro

Gruppi funzionali in un progetto di migrazione responsabili di una serie specifica di attività. Ogni flusso di lavoro è indipendente ma supporta gli altri flussi di lavoro del progetto. Ad esempio, il flusso di lavoro del portfolio è responsabile della definizione delle priorità delle applicazioni, della pianificazione delle ondate e della raccolta dei metadati di migrazione. Il flusso di lavoro del portfolio fornisce queste risorse al flusso di lavoro di migrazione, che quindi migra i server e le applicazioni.

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

Un modello di storage che scrive i dati una sola volta e ne impedisce l'eliminazione o la modifica. Gli utenti autorizzati possono leggere i dati tutte le volte che è necessario, ma non possono modificarli. Questa infrastruttura di archiviazione dei dati è considerata immutabile.

Z

exploit zero-day

Un attacco, in genere malware, che sfrutta una vulnerabilità zero-day.

vulnerabilità zero-day

Un difetto o una vulnerabilità assoluta in un sistema di produzione. Gli autori delle minacce possono utilizzare questo tipo di vulnerabilità per attaccare il sistema. Gli sviluppatori vengono spesso a conoscenza della vulnerabilità causata dall'attacco.

prompt zero-shot

Fornire a un LLM le istruzioni per eseguire un'attività ma non esempi (immagini) che possano aiutarla. Il LLM deve utilizzare le sue conoscenze pre-addestrate per gestire l'attività. L'efficacia del prompt zero-shot dipende dalla complessità dell'attività e dalla qualità del prompt. Vedi anche few-shot prompting.

applicazione zombie

Un'applicazione che prevede un utilizzo CPU e memoria inferiore al 5%. In un progetto di migrazione, è normale ritirare queste applicazioni.

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.