Investire nell'ingegneria del caos come necessità strategica

AWS Guida prescrittiva

AWS Guida prescrittiva: Investire nell'ingegneria del caos come necessità strategica

Table of Contents

Investire nell'ingegneria del caos come necessità strategica

Adrian Hornsby, Amazon Web Services

Gennaio 2025 (cronologia del documento)

Le pratiche di ingegneria del caos utilizzano interruzioni controllate per identificare i problemi del sistema e le opportunità per prevenire interruzioni e altri incidenti. L'ingegneria del caos è diventata essenziale per migliorare i sistemi resilienti, ma un'adozione diffusa incontra ostacoli legati a idee sbagliate, resistenza culturale, risorse e come quantificare il valore aziendale. La definizione degli obiettivi iniziali aiuta a dare il via alle iniziative di ingegneria del caos, mentre la quantificazione del ritorno sull'investimento (ROI) giustifica investimenti continui, soprattutto in un contesto di pressioni economiche.

Questo documento strategico delinea un approccio olistico per acquisire sia miglioramenti operativi quantitativi che vantaggi organizzativi qualitativi. L'obiettivo finale è considerare l'ingegneria del caos come una necessità strategica simile alla sicurezza informatica e non come un esercizio continuo di giustificazione dei costi.

I costi dei tempi di inattività e l'emergere dell'ingegneria del caos

L'Information Technology Intelligence Consulting (ITIC) stima che il 90% delle aziende debba affrontare costi superiori a 300.000 dollari per ora di inattività, mentre il 41% supera i 1,5 milioni di dollari all'ora. Oltre alla perdita immediata di fatturato, i tempi di inattività possono portare a problemi a lungo termine, tra cui errori di conformità, abbassamento dei prezzi delle azioni, significativi costi di mitigazione e persino danni al marchio.

Sebbene i tempi di inattività siano comunemente associati ai sistemi online che generano entrate, l'impatto negativo si estende ben oltre. Tutte le grandi aziende e organizzazioni, indipendentemente dal loro modello di fatturato principale, si affidano in modo fondamentale alla disponibilità dei propri sistemi interni, come le risorse umane e le buste paga.

I tempi di inattività che influiscono su questi servizi interni fondamentali possono inibire la capacità di un'azienda di funzionare, con conseguenti sostanziali interruzioni operative e ripercussioni finanziarie. I problemi che ne derivano possono includere quanto segue:

- Ritardi nel pagamento di dipendenti e fornitori
- Impossibilità di elaborare gli ordini o le transazioni dei clienti
- Violazioni di dati sensibili consentite da sistemi di sicurezza compromessi
- Perdita di produttività e opportunità di guadagno
- Sanzioni normative in caso di non conformità
- Danni alla reputazione del marchio

L'ingegneria del caos introduce intenzionalmente interruzioni controllate. L'uso dell'ingegneria del caos per comprendere o verificare la risposta del sistema ai guasti è diventata una pratica fondamentale per migliorare la resilienza del sistema. L'ingegneria del caos consente all'organizzazione di scoprire in modo proattivo i problemi, convalidare i meccanismi di resilienza e, in ultima analisi, ridurre il rischio di tempi di inattività non pianificati e i relativi costi. I vantaggi dell'ingegneria del caos includono quanto segue:

- Esposizione del debito tecnico
- Esercizio dei muscoli operativi
- Rafforzare la fiducia nei sistemi

- Identificazione dei punti di guasto
- Migliorare il monitoraggio e l'osservabilità
- Sostenere l'apprendimento basato sugli esperimenti
- Offrire una maggiore resilienza per ridurre i tempi di inattività

Man mano che i sistemi diventano più complessi e le aspettative dei clienti aumentano, l'ingegneria del caos sta diventando sempre più importante. Gartner consiglia l'ingegneria del caos come pratica fondamentale per le organizzazioni per ridurre i tempi di inattività non pianificati e migliorare la resilienza.

Le sfide di adozione dell'ingegneria del caos

Sebbene l'ingegneria del caos sia una pratica sempre più importante per migliorare la resilienza dei sistemi, la sua adozione può incontrare i seguenti ostacoli:

- Percezioni errate sul rischio – Un'errata percezione comune è che l'ingegneria del caos venga condotta solo in ambienti di produzione, il che porta a temere un rischio eccessivo. Questa percezione deriva da una mancanza di comprensione della natura sistematica e controllata delle pratiche di ingegneria del caos. Come indicato nel AWS Well-Architected Framework, esegui prima la simulazione dei guasti in un ambiente non di produzione.
- Valore aziendale a lungo termine – I vantaggi di Chaos engineering si accumulano gradualmente, rendendo difficile quantificare il valore aziendale e giustificare l'investimento iniziale. Il ROI più lento rende difficile per le organizzazioni stabilire le priorità e attenersi all'ingegneria del caos.
- Lacune nelle competenze e nelle competenze – L'ingegneria del caos richiede un insieme unico di competenze e competenze che potrebbero non essere immediatamente disponibili all'interno dell'organizzazione. Lo sviluppo o l'acquisizione di queste competenze può rappresentare un ostacolo significativo, soprattutto per le organizzazioni che sono nuove alla pratica e quelle con risorse limitate.

Il resto di questo documento strategico si concentrerà principalmente sulla seconda sfida, che consiste nel dimostrare il valore aziendale dell'ingegneria del caos.

Gli effetti cumulativi dell'ingegneria del caos

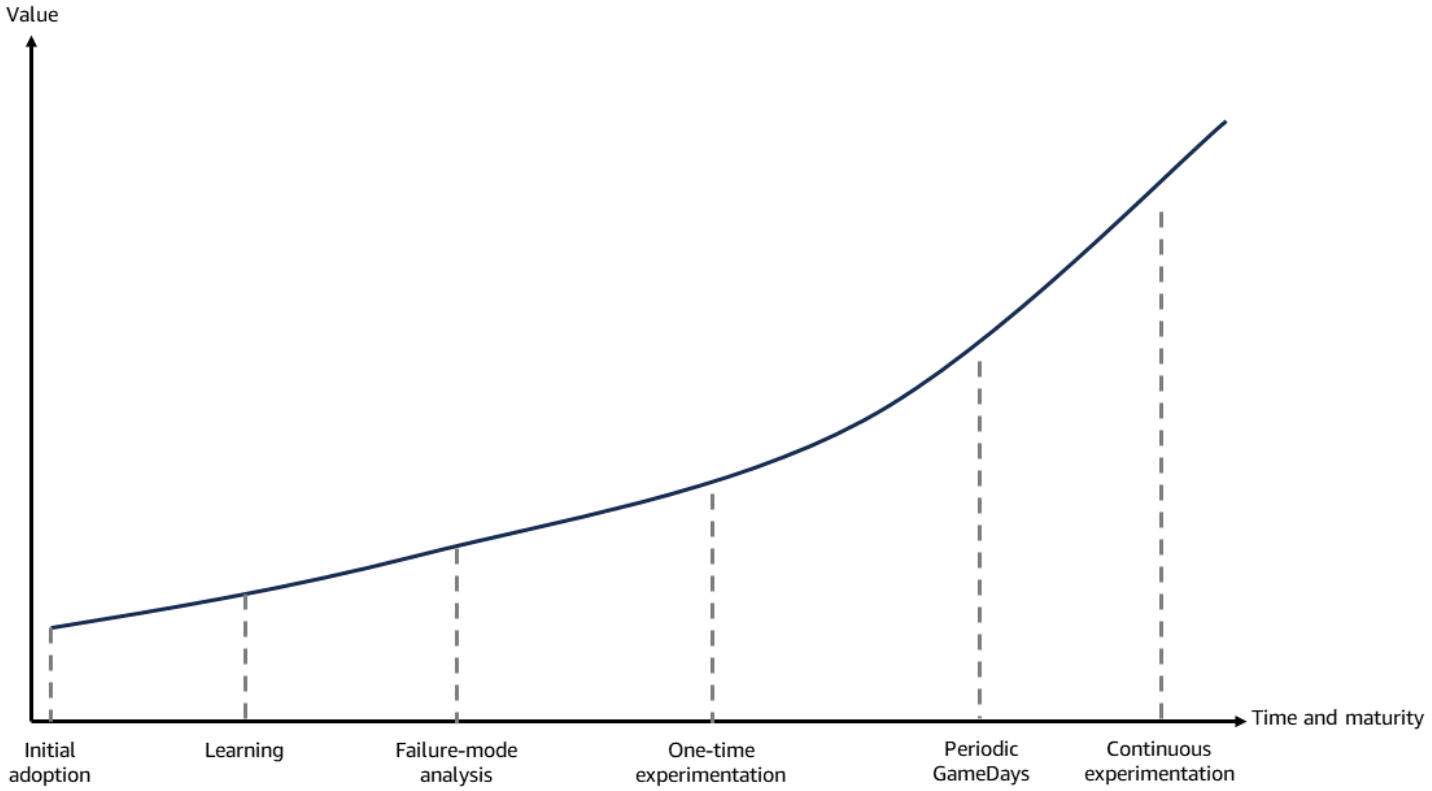
A differenza dei progetti tecnologici tradizionali con date di inizio e fine ben definite, l'ingegneria del caos è una pratica continua di apprendimento continuo e miglioramento continuo della resilienza del sistema. I vantaggi dell'ingegneria del caos si aggravano nel tempo.

Man mano che i sistemi si evolvono e diventano più complessi, emergono nuove modalità di errore. Sono necessari ulteriori esperimenti sul caos per identificare potenziali problemi. La risoluzione di un problema può richiedere mesi, soprattutto nelle grandi aziende con sistemi e processi complessi o quando i guasti sono di proprietà di fornitori di servizi esterni.

Il cambiamento culturale verso l'accettazione del fallimento come opportunità di apprendimento e miglioramento cresce nel corso degli anni e diventa radicato nell'organizzazione. Gli investimenti nell'automazione degli esperimenti di ingegneria del caos e nello sviluppo di strumenti di supporto continuano a semplificare e migliorare la pratica dell'ingegneria del caos. Lo sviluppo di questa conoscenza istituzionale e della comprensione della resilienza del sistema è un processo graduale che si accumula nel tempo. Le conoscenze, i processi e gli strumenti sviluppati attraverso l'ingegneria del caos aumentano di valore man mano che la pratica matura insieme ai sistemi in continua evoluzione.

Il diagramma seguente mostra come il valore aumenta nel tempo man mano che l'adozione del caos progredisce attraverso le seguenti fasi:

- Adozione iniziale
- Apprendimento
- Analisi in modalità di errore
- Esperimenti una tantum
- Periodico GameDays
- Sperimentazione continua



Come illustrato nel diagramma, i vantaggi dell'ingegneria del caos spesso iniziano prima che qualsiasi guasto venga iniettato nel sistema. Il processo di pianificazione e progettazione degli esperimenti sul caos fornisce di per sé un valore immediato. L'identificazione di potenziali scenari di fallimento, singoli punti di errore e aree di incertezza nel sistema porta a miglioramenti.

Ad esempio, annotare gli scenari di errore e discutere dei potenziali effetti a cascata, un processo chiamato analisi della modalità e degli effetti di errore (FMEA), aiuta a scoprire punti deboli o lacune evidenti che potrebbero essere stati trascurati. L'organizzazione può affrontare questi problemi in modo proattivo, anche prima di sottoporre il sistema a interruzioni intenzionali. Per ulteriori informazioni, consulta il framework di analisi della resilienza.

Inoltre, la maggiore attenzione all'osservabilità e al monitoraggio del sistema, che spesso accompagna le iniziative di ingegneria del caos, inizia a fornire vantaggi fin da subito. Migliorare la visibilità sul comportamento del sistema e sulle modalità di errore aiuta il team a comprendere meglio le normali condizioni operative del sistema. Una maggiore visibilità aiuta anche il team a capire in che modo le condizioni operative peggiorano, si adattano e si guastano quando vengono spinte al limite.

Sia la modalità sperimentale una tantum che quella periodica sono approcci più manuali rispetto alla GameDay modalità di sperimentazione continua. Richiedono un processo più pratico ed esplorativo,

in cui gli ingegneri modellano e perfezionano attivamente le ipotesi attraverso le loro osservazioni ed esperimenti.

La modalità di sperimentazione continua è, invece, di natura più automatizzata. Questa modalità si concentra sull'esecuzione di ipotesi approvate e convalidate in modo controllato e iterativo. Utilizza l'automazione e l'integrazione nel processo di sviluppo attraverso una pipeline dedicata al caos per garantire esperimenti coerenti e ripetibili.

Iniziative di ingegneria del caos di base

Il percorso di ingegneria del caos spesso inizia a livello di base, dove i team di ingegneri identificano le esigenze e iniziano a sperimentare l'ingegneria del caos in modo indipendente.

In questo approccio di base, i team sperimentano, apprendono e perfezionano le loro pratiche di ingegneria del caos. Il valore dell'ingegneria del caos può essere dimostrato attraverso i seguenti risultati tangibili:

- Incidenti ridotti
- Migliore osservabilità
- Tempi di ripristino più rapidi
- Resilienza del sistema migliorata e continua

Le iniziative di ingegneria del caos di base emergono in genere in condizioni organizzative specifiche. Richiedono un ambiente con un alto grado di autonomia ingegneristica, in cui i team abbiano la libertà di sperimentare e innovare senza eccessive barriere burocratiche. L'esperienza locale nell'ingegneria della resilienza o nei sistemi distribuiti è fondamentale, perché fornisce le basi tecniche per comprendere e implementare esperimenti di caos. Soprattutto, queste iniziative spesso si basano su campioni del caos, individui appassionati che comprendono il valore dell'ingegneria del caos. I campioni del caos sono disposti a sostenere l'adozione dell'ingegneria del caos, a istruire i propri colleghi e a guidare i primi esperimenti. Senza libertà organizzativa, competenze tecniche e sostenitori motivati, le iniziative di ingegneria del caos di base raramente mettono radici, indipendentemente dai loro potenziali benefici.

Il ruolo degli obiettivi nell'adozione dell'ingegneria del caos

È normale che gli obiettivi iniziali emergano in modo organico dagli sforzi di base di ingegneria del caos all'interno di un'organizzazione. Spinti dalla necessità di risolvere i propri problemi ricorrenti, questi team o gruppi spesso esplorano pratiche di ingegneria del caos senza l'approvazione esplicita o la definizione di priorità da parte dei livelli superiori.

I team possono utilizzare questi risultati per sviluppare argomentazioni convincenti a favore di un'adozione più ampia da parte delle organizzazioni, diventando di fatto un banco di prova per altri team.

Dopo che i vantaggi derivanti dagli sforzi di base diventano troppo importanti per essere ignorati, questi team possono elevare i propri sforzi e le proprie conoscenze alla leadership e fissare obiettivi. Questa maggiore visibilità può facilitare l'adozione di obiettivi di resilienza a livello di organizzazione e portare al supporto e alle risorse necessari per l'implementazione dell'ingegneria del caos.

Gli obiettivi, in particolare quelli guidati dalla leadership e stabiliti in risposta a interruzioni significative, svolgono un ruolo cruciale nel catalizzare l'adozione di pratiche di ingegneria del caos. I tipi più comuni di obiettivi includono i seguenti:

- Obiettivi di disponibilità per identificare e ridurre i singoli punti di errore (SPOF)
- Obiettivi di ripristino dei servizi volti a migliorare la capacità di ripristino in caso di interruzioni o guasti
- Obiettivi relativi all'esperienza utente per soddisfare obiettivi specifici relativi ai livelli di servizio () SLOs
- Obiettivi basati su metriche per monitorare i progressi nella mitigazione dei rischi di disponibilità noti e nell'implementazione delle misure di resilienza consigliate
- Obiettivi normativi e di conformità per dimostrare la resilienza operativa

Per ulteriori informazioni su alcuni di questi tipi di obiettivi e su come Amazon e altre organizzazioni hanno utilizzato gli obiettivi durante l'adozione di Chaos Engineering, consulta l'Appendice A.

Questi obiettivi servono come giustificazione convincente e forniscono un approccio mirato e attuabile per promuovere l'adozione dell'ingegneria del caos. All'inizio, gli obiettivi fungono da indicatore per le metriche tradizionali del ROI. Gli obiettivi offrono una motivazione convincente quando i calcoli quantificabili del ROI in termini di resilienza potrebbero essere difficili da ottenere. Senza tali obiettivi

nelle prime fasi di adozione, la pratica dell'ingegneria del caos rischia di non riuscire a dimostrare la propria efficacia e ad ottenere un più ampio consenso organizzativo.

Il passaggio dagli obiettivi alla misurazione del ROI

Man mano che le pratiche maturano e gli obiettivi iniziali vengono raggiunti, alla fine l'attenzione si sposta dalla definizione degli obiettivi alla quantificazione dei vantaggi finanziari tangibili dell'ingegneria del caos: il ritorno sull'investimento (ROI). Il cambiamento deriva da due ragioni principali:

- Considerazioni economiche
- Preservare l'esperienza e la fiducia dei clienti

Considerazioni economiche

In tempi di crescita economica e finanze sane, spesso le aziende non hanno bisogno di ampie giustificazioni per fissare obiettivi specifici per le strategie di ingegneria del caos. Tuttavia, i cambiamenti nel panorama finanziario hanno portato molte organizzazioni a rivalutare i propri investimenti e le implementazioni di ingegneria del caos devono fornire un ROI quantificato.

Queste aziende hanno ora il compito di definire metriche chiare e tradizionali del ROI per dimostrare il valore e l'impatto delle pratiche di ingegneria del caos. Questa sfida è ulteriormente complicata dal paradosso della prevenzione. Il paradosso della prevenzione si verifica quando una prevenzione efficace degli incidenti rende più difficile giustificare l'investimento, perché le parti interessate tendono a sottovalutare le catastrofi evitate. Anche le organizzazioni con una cultura profondamente radicata dell'eccellenza operativa devono far fronte alla pressione di utilizzare le metriche del ROI per giustificare l'adozione continua dell'ingegneria del caos.

Preservare l'esperienza e la fiducia dei clienti

Sostenere la resilienza basata sugli obiettivi può essere difficile a lungo termine. Dopo aver raggiunto un obiettivo iniziale, come il raggiungimento di un obiettivo relativo ai tempi di ripristino, diventa difficile giustificare continui investimenti nella progettazione del caos fino alla prossima grave interruzione. Il flusso e il calo degli investimenti creano un ciclo reattivo a denti stretti. Per ogni nuova interruzione, gli investimenti nella resilienza aumentano con un nuovo obiettivo: affrontarne la causa principale. Una volta raggiunto il nuovo obiettivo, gli investimenti diminuiscono fino all'incidente successivo, riavviando il ciclo reattivo.

Le interruzioni alla base di questo approccio reattivo hanno un impatto negativo sui clienti. La domanda chiave: quante interruzioni gravi tollereranno i clienti prima di abbandonare un fornitore di servizi a favore di un concorrente più resiliente?

Quantificazione del ROI dell'ingegneria del caos

Attualmente, pochissime risorse pubblicate forniscono metodologie complete o dati reali per quantificare il ritorno sull'investimento (ROI) a lungo termine per l'ingegneria del caos.

Nel paper The Business Case for Chaos Engineering, Netflix offre una valida equazione per il calcolo del ROI dell'ingegneria del caos. Questa equazione fornisce un punto di partenza per le organizzazioni che intraprendono il loro percorso di ingegneria del caos.

L'equazione richiede una stima accurata dei costi di quanto segue:

- Interruzioni prevenibili e non prevenibili
- Costi di implementazione del programma di ingegneria del caos
- Costi dei danni causati dal caos

I danni causati dal caos si riferiscono all'impatto negativo o alla perturbazione causati dall'introduzione deliberata di guasti o condizioni turbolente in un sistema nell'ambito di esperimenti di ingegneria del caos. L'equazione richiede la stima dei costi delle interruzioni evitabili e non evitabili, dei costi di implementazione dei programmi di ingegneria del caos e dei danni causati dal caos.

Determinare con certezza quali problemi avrebbero potuto essere evitati con un programma di ingegneria del caos è un compito difficile. Richiede un'analisi ipotetica che preveda l'analisi delle cause profonde dei problemi e la speculazione su come gli esperimenti di ingegneria del caos avrebbero potuto contribuire a identificarli. Questa analisi è impegnativa perché i sistemi moderni sono estremamente complessi, con numerose interdipendenze e interazioni tra vari componenti, servizi e librerie di terze parti. Inoltre, i guasti nei sistemi sono spesso non deterministici e le condizioni che causano i guasti possono essere difficili da comprendere appieno con il senno di poi.

Sebbene l'approccio suggerito da Netflix presenti alcune limitazioni, rappresenta una buona base per le organizzazioni che iniziano a esplorare l'ingegneria del caos. L'equazione può aiutarvi a stimare i costi e i potenziali benefici, aiutandovi a prendere decisioni sull'implementazione di un programma di questo tipo. Tuttavia, man mano che le organizzazioni progrediscono ulteriormente nel loro percorso di ingegneria del caos, è importante ampliare la valutazione del ROI per incorporare una prospettiva più olistica.

Questo approccio olistico non solo coglierà i vantaggi diretti della riduzione delle interruzioni e dei costi di progettazione, ma evidenzierà anche gli effetti trasformativi a lungo termine sulla resilienza

complessiva dell'organizzazione. Racchiude i vantaggi combinati e gli effetti organizzativi più ampi dell'ingegneria del caos per fornire una rappresentazione più accurata del vero valore e dell'impatto dell'ingegneria del caos.

Un approccio olistico alla quantificazione del ROI

Una valutazione olistica del ROI deve tenere conto non solo delle misure quantitative ma anche dei fattori qualitativi. L'approccio olistico richiede dati reali provenienti da organizzazioni che praticano l'ingegneria del caos su larga scala per periodi di tempo più lunghi. Puoi utilizzare i dati a partire dai progetti e dagli obiettivi di base attraverso qualsiasi dato sul ROI con approccio equazionale che hai raccolto.

Le misure quantitative si concentrano su quantità o frequenze. Le misurazioni sono oggettive e possono essere analizzate statisticamente. Gli esempi includono sondaggi, esperimenti e analisi dei dati. Le misure quantitative possono includere quanto segue:

- Metriche degli incidenti
- Costi
- Miglioramenti
- Conformità
- Tassi di adozione
- La soddisfazione del cliente

Il monitoraggio delle misure quantitative può dimostrare i vantaggi operativi diretti dell'ingegneria del caos.

Le misure qualitative sono descrittive e si concentrano sulla comprensione di esperienze e opinioni. Spesso sono soggettive e non possono essere facilmente misurate numericamente. Per quanto riguarda l'ingegneria del caos, le misure qualitative tengono conto degli impatti organizzativi più ampi. Le misure qualitative possono includere quanto segue:

- Fiducia dei dipendenti
- Cambiamento culturale
- Collaborazione
- Efficacia della formazione
- Conservazione dei talenti

- La reputazione del marchio
- Vantaggio competitivo

Considerando sia gli impatti finanziari quantitativi che i vantaggi organizzativi qualitativi, è possibile prendere decisioni più informate sui continui investimenti nell'ingegneria del caos, promuovendo al contempo una cultura della resilienza.

Per ulteriori informazioni su queste misure e sul relativo quadro di classificazione degli incidenti, vedere l'Appendice B e l'Appendice C.

La transizione dal ROI all'ingegneria del caos come necessità strategica

Sebbene sia allettante monitorare il ROI, le difficoltà legate alla misurazione del valore dell'ingegneria del caos spesso portano le organizzazioni a dare priorità alle efficienze immediate e a breve termine rispetto agli investimenti strategici in materia di resilienza. Questo approccio trascura l'ingegneria del caos come fattore chiave della resilienza e i vantaggi competitivi derivanti dall'evitare le interruzioni. Il vero valore dell'ingegneria del caos sta nella prevenzione di futuri fallimenti. L'ingegneria del caos supporta la continuità aziendale a lungo termine.

Invece di concentrarti sul ROI, considera l'ingegneria del caos come la sicurezza informatica. Come spiegato nell'articolo di Forbes La sicurezza informatica come investimento strategico: come l'ottimizzazione del ROI può portare a un futuro più sicuro, la sicurezza informatica non dovrebbe essere vista come un centro di costo o una spesa obbligatoria per le organizzazioni, perché questa mentalità non riesce a riconoscere il valore strategico che solide misure di sicurezza informatica possono fornire nel tempo. L'autore sostiene invece che cambiando prospettiva per trattare la sicurezza informatica come un investimento a lungo termine che genera vantaggi competitivi, le organizzazioni possono sbloccare nuove strade per l'innovazione, l'efficienza operativa e la differenziazione all'interno dei rispettivi mercati. Adottando questo approccio, l'autore conclude che i Chief Information Security Officer () possono garantire meglio il consenso e i finanziamenti dei dirigenti. CISOs Possono quindi posizionare le proprie aziende in modo da superare i concorrenti in un panorama informatico sempre più rischioso. Questa creazione di valore strategico a lungo termine della sicurezza informatica è parallela ai continui miglioramenti inerenti alle pratiche di ingegneria del caos.

Mentre la sicurezza salvaguarda la capacità di un'organizzazione di gestire e proteggere le risorse, l'ingegneria del caos aiuta a garantire la disponibilità, l'affidabilità e la recuperabilità dei sistemi e dei servizi principali. Per realizzare valore e vantaggio competitivo a lungo termine, trattate l'ingegneria del caos come una capacità fondamentale e un imperativo strategico, non come un'iniziativa che richiede una giustificazione costante.

Il diagramma seguente mostra l'evoluzione dell'ingegneria del caos dalla base agli obiettivi e al ROI, fino a diventare una strategia.

A livello di base, i singoli team in genere sperimentano in modo indipendente, guidati dalle esigenze locali. Questi esperimenti sono promossi da ingegneri appassionati che dimostrano il loro valore riducendo gli incidenti e migliorando l'osservabilità.

Quando questi sforzi si rivelano efficaci, i team possono elevare il loro apprendimento alla leadership. Con questa visibilità, gli sforzi passano a una fase basata sugli obiettivi. L'organizzazione stabilisce obiettivi formali per la resilienza e il recupero, supportati da risorse e supporto per un'implementazione più ampia.

Infine, l'ingegneria del caos matura oltre a richiedere una costante giustificazione del ROI per essere riconosciuta come una necessità strategica, simile alla sicurezza informatica. In questa fase, l'ingegneria del caos diventa completamente integrata nei processi organizzativi. L'implementazione si concentra sulla resilienza a lungo termine piuttosto che sulle metriche a breve termine. L'ingegneria del caos è considerata una capacità fondamentale essenziale per mantenere il vantaggio competitivo e la fiducia dei clienti.

Integrazione dell'ingegneria del caos nella propria organizzazione

Per elevare l'ingegneria del caos allo stesso livello di importanza della sicurezza, prendete in considerazione i seguenti suggerimenti:

- Far diventare l'ingegneria del caos una pratica non negoziabile – Proprio come la sicurezza informatica è considerata un requisito fondamentale per le organizzazioni, l'ingegneria del caos è considerata una pratica obbligatoria per garantire la resilienza e l'affidabilità del sistema. Integra l'ingegneria del caos nei processi, negli strumenti e nella cultura della tua organizzazione, anziché considerarla un'attività facoltativa o discrezionale. Per ulteriori informazioni, consulta la guida al framework Resilience Lifecycle.
- Consenso e supporto sicuri a livello dirigenziale – Come per le iniziative di sicurezza, le iniziative di ingegneria del caos devono avere il consenso e il supporto attivo dei dirigenti. Ciò include l'allocazione di risorse, budget e personale dedicati per implementare e sostenere le pratiche di ingegneria del caos in tutta l'organizzazione.

- Implementa la governance e la supervisione – Analogamente a un CISO e a un framework di governance della sicurezza, istituisci un team dedicato alla progettazione del caos o un Chief Resilience Officer. Questo team o ruolo è responsabile della supervisione e del coordinamento delle attività di ingegneria del caos tra diversi team e unità aziendali.
- Integrate l'ingegneria del caos nei cicli di sviluppo e operativi – Proprio come le pratiche di sicurezza sono integrate nei processi di sviluppo e distribuzione del software, fate dell'ingegneria del caos una parte integrante del ciclo di vita dello sviluppo e della distribuzione del software.
- Conduci regolarmente esercitazioni e simulazioni di ingegneria del caos – Analogamente alle simulazioni di violazioni della sicurezza e alle esercitazioni di risposta agli incidenti, conduci regolarmente esperimenti di ingegneria del caos per convalidare le capacità di risposta agli incidenti e identificare potenziali punti ciechi in modo proattivo.
- Usa l'ingegneria del caos per gestire i runbook – Analogamente alle revisioni di sicurezza, utilizza esperimenti di ingegneria del caos per convalidare l'efficacia e l'accuratezza dei runbook per la risposta e il ripristino degli incidenti. Inoltre, gli esperimenti di ingegneria del caos possono fungere da simulazioni realistiche per consentire agli ingegneri in servizio di esercitarsi nell'esecuzione delle procedure di runbook. Le simulazioni aiutano gli ingegneri a mantenere la memoria muscolare operativa e la preparazione per gestire gli incidenti del mondo reale.
- Promuovi una cultura della resilienza – Come per la formazione sulla sensibilizzazione alla sicurezza, investi nella formazione sull'ingegneria del caos e in iniziative di condivisione delle conoscenze per promuovere una cultura della resilienza. Includi programmi di formazione, collaborazione interfunzionale e incentivi per i team che adottano pratiche di ingegneria del caos.
- Misura e riporta le metriche di resilienza – Monitora regolarmente le metriche di resilienza e segnalale alle parti interessate. Utilizza le metriche quantitative e qualitative discusse in questo documento come punto di partenza.
- Considera la resilienza come un vantaggio competitivo – Le misure di sicurezza informatica possono fornire un vantaggio competitivo. Allo stesso modo, considera le tue capacità di ingegneria del caos e resilienza come un elemento di differenziazione che ti aiuta a offrire servizi più affidabili e affidabili ai tuoi clienti.

Ottenere il consenso dei dirigenti

L'ingegneria del caos spesso non ha una chiara responsabilità nell'ambito delle responsabilità tradizionali dei vertici aziendali. Il CEO si preoccupa della crescita, della redditività e della leadership di mercato. Il CFO si concentra sulla performance finanziaria, sul controllo dei costi e sulla gestione

del rischio. Il CTO dà priorità alla strategia tecnologica, alle roadmap dei prodotti e all'eccellenza ingegneristica. Il CISO supervisiona la sicurezza e la conformità.

Poiché nessun dirigente è realmente responsabile della resilienza, spesso è difficile ottenere consenso e supporto. Tuttavia, i guasti del sistema influiscono sui ricavi, sulla soddisfazione dei clienti e sulla reputazione del marchio, che sono preoccupazioni per CEO e CFO. Il CTO e il CISO hanno il compito di implementare misure di resilienza, ma potrebbero non avere un mandato organizzativo. Questa ambiguità può ostacolare gli investimenti strategici e l'allineamento dell'organizzazione verso una strategia di resilienza comune.

Questa ambiguità rende inoltre difficile ottenere il consenso dei dirigenti per iniziative di resilienza come l'ingegneria del caos. Dopotutto, i dirigenti di livello C si destreggiano tra una moltitudine di priorità strategiche: crescita, innovazione, esperienza del cliente, conformità e altro ancora.

Per comunicare efficacemente il valore dell'ingegneria del caos ai dirigenti di livello C, prendete in considerazione i seguenti approcci:

- Determinate le preoccupazioni principali e i fattori decisionali dei vostri dirigenti di alto livello.

  Ad esempio, i dirigenti della C-suite sono preoccupati per il tasso di abbandono dei clienti, la conformità alle normative, la riduzione dei costi o le pressioni della concorrenza? Posiziona l'ingegneria del caos come un moltiplicatore di forza in linea con le sfide e gli obiettivi unici dell'azienda.
- Identifica obiettivi e risultati strategici condivisi.

  In che modo la vostra strategia di ingegneria del caos supporta la strategia di crescita complessiva dell'organizzazione, l'esperienza del cliente, le opportunità di mercato e l'efficienza operativa? Assegna priorità alle iniziative in base agli obiettivi, all'impatto aziendale, al ROI e al rischio di non intraprendere tali iniziative.
- Comunica l'efficacia della tua strategia di ingegneria del caos in termini quantificabili utilizzando indicatori chiave di resilienza.

  Inizia con questi quattro indicatori chiave di resilienza: disponibilità, tempo di rilevamento, tempo di risposta e tempo di ripristino. Collegali direttamente a risultati aziendali come entrate, risparmi sui costi e reputazione del marchio.
- Non perderti nei dettagli tecnici.

Concentrati sul sentiment generale e sull'impatto aziendale misurabile. I dirigenti si preoccupano dei risultati che favoriscono la crescita, aumentano la fiducia dei clienti e promuovono l'innovazione.

Il paradosso della prevenzione

Quando i guasti vengono mitigati con successo prima che si manifestino, diventa difficile convincere le parti interessate del valore e della necessità delle misure preventive adottate. Questo fenomeno è noto come paradosso della prevenzione. Il paradosso della prevenzione è il principale ostacolo all'integrazione dell'ingegneria del caos come necessità strategica e deriva dai pregiudizi intrinseci della cognizione umana.

Il bug Y2K è un ottimo esempio di questo paradosso. Anni di preparazione e miliardi di dollari sono stati investiti nell'aggiornamento dei sistemi informatici in tutto il mondo. Tuttavia, l'agevole transizione verso il 2000 è stata interpretata da molti come una dimostrazione della natura esagerata delle preoccupazioni relative all'Y2K. Il successo degli sforzi di prevenzione intrapresi è stato raramente riconosciuto.

Questo paradosso della prevenzione continua a rappresentare una sfida per le organizzazioni che oggi investono nell'ingegneria del caos. Quando potenziali interruzioni vengono evitate con successo attraverso misure proattive, la stessa assenza di catastrofi può paradossalmente rendere difficile giustificare le risorse spese per la prevenzione.

La causa principale di questo fenomeno risiede nel modo in cui le nostre menti sono programmate per elaborare le informazioni. I processi cognitivi umani sono orientati a rispondere e ricordare eventi reali e risultati visibili. Quando si previene un disastro, non c'è una narrazione drammatica a cui aggrapparsi o condividere. Un altro aspetto del paradosso della prevenzione è il pregiudizio col senno di poi. Dopo un mancato evento, le persone tendono a concludere che non è successo nulla, quindi non è stato un vero problema. La possibilità che le precauzioni appropriate abbiano impedito un problema reale non è riconosciuta. Questo punto cieco psicologico crea una sfida perpetua per le organizzazioni. Più riuscite a prevenire e a mantenere la resilienza, più a posteriori i vostri sforzi sembrano superflui.

Per risolvere il paradosso della prevenzione, l'organizzazione può adottare misure specifiche per rendere visibile, misurabile e valorizzata l'opera invisibile di prevenzione. I potenziali passaggi includono quanto segue:

- Documenta e simula cosa sarebbe potuto succedere senza misure preventive.

- Racconta storie di eventi in cui le misure preventive hanno evitato potenziali disastri.
- Indicate le organizzazioni simili che non si sono preparate e che ne hanno subito le conseguenze.
- Presentate i costi di prevenzione nel contesto dei potenziali impatti che stanno prevenendo.
- Suddividi gli sforzi di prevenzione in traguardi e risultati visibili.
- Costruisci una memoria istituzionale sul motivo per cui esistono le misure preventive e sulla loro importanza storica.
- Istruisci regolarmente le parti interessate sul valore della resilienza e delle pratiche di ingegneria del caos.

Conclusioni

L'ingegneria del caos è un imperativo strategico per le organizzazioni. Anche se il percorso di adozione potrebbe dover affrontare sfide come idee sbagliate, resistenze culturali e limiti di risorse, la definizione di obiettivi chiari e orientati alla leadership può catalizzare il processo. Man mano che le pratiche maturano, quantificate il ritorno sull'investimento attraverso un approccio olistico che tenga conto sia dei miglioramenti operativi quantitativi che dei vantaggi organizzativi qualitativi. L'approccio olistico è particolarmente importante durante le pressioni economiche.

Per trasformare questa necessità strategica in realtà, iniziate a valutare l'attuale livello di maturità della vostra organizzazione. La tua organizzazione si trova nella fase di sperimentazione di base, nella fase basata sugli obiettivi o in una fase intermedia? Sulla base di questa valutazione, crea una tabella di marcia personalizzata per realizzare quanto segue:

- Stabilisci una governance ingegneristica del caos (ad esempio, nomina un Chief Resilience Officer).
- Integra le pratiche legate al caos nei flussi di lavoro di sviluppo.
- Implementa programmi di formazione regolari.
- Sviluppa metriche di resilienza complete.

Questa trasformazione non avverrà dall'oggi al domani. Tuttavia, l'adozione di queste misure concrete, garantendo al contempo un supporto esecutivo continuo, contribuirà a portare l'ingegneria del caos allo stesso livello strategico della sicurezza informatica. Analogamente alla sicurezza informatica, l'ingegneria del caos può diventare parte integrante del DNA e dei processi operativi dell'organizzazione.

Risorse

- Risultati del sondaggio ITIC 2021 Global Server Hardware e Server OS sull'affidabilità
- Il caso aziendale dell'ingegneria del caos
- La sicurezza informatica come investimento strategico: come l'ottimizzazione del ROI può portare a un futuro più sicuro
- La guida all'ingegneria del caos per i leader di I&O
- Come usare il punteggio AWS Resilience Hub
- Implementazione degli esperimenti consigliati utilizzando la console AWS Resilience Hub

Appendice A – Tipi di obiettivi per l'ingegneria del caos

Le seguenti descrizioni dei tipi di obiettivi includono esempi reali di come Amazon e altre organizzazioni hanno progettato obiettivi per l'ingegneria del caos.

Obiettivi di architettura resiliente

Uno dei fattori iniziali per l'adozione dell'ingegneria del caos è l'identificazione e la riduzione dei singoli punti di errore (SPOF) tra sistemi e infrastrutture. Gli obiettivi sono fissati per convalidare la resilienza dei sistemi e delle architetture critiche, in particolare per nuovi servizi o applicazioni.

Gli obiettivi dell'architettura resiliente prevedono l'esecuzione di esperimenti di caos che simulano i guasti nelle dipendenze dei servizi. Gli esperimenti confermano se i timeout, i nuovi tentativi, il comportamento di memorizzazione nella cache e le configurazioni degli interruttori automatici funzionano correttamente. Questi esperimenti aiutano a scoprire i problemi da risolvere, prevenendo incidenti che possono avere ripercussioni sui clienti. Per un esempio, consulta Creazione di servizi resilienti in Prime Video con Chaos Engineering.

Obiettivi di ripristino dei servizi

Gli obiettivi di ripristino dei servizi si concentrano sul miglioramento della capacità di ripristino in seguito a interruzioni operative o guasti dell'infrastruttura. Ad esempio, l'organizzazione potrebbe mirare a raggiungere un obiettivo RTO (Recovery Time Objective) specifico per i servizi principali in caso di interruzione. I team possono progettare esperimenti di caos per convalidare e ottimizzare le strategie di evacuazione, i meccanismi di failover e i processi di ripristino automatizzati. Le ottimizzazioni riducono in ultima analisi il tempo necessario per il ripristino del servizio. Per un esempio, vedi AWS Lambda: under-the-hood Resilience.

Obiettivi relativi all'esperienza utente

Mantenere un'esperienza utente coerente e affidabile è fondamentale, specialmente durante i periodi di traffico intenso o gli eventi critici. In questi casi, stabilite obiettivi incentrati sul raggiungimento di obiettivi specifici a livello di servizio (). SLOs Questo approccio incentrato sul cliente garantisce che gli sforzi di resilienza siano direttamente allineati all'offerta di un'esperienza utente superiore, anche in caso di guasti o condizioni degradate. Per un esempio, consulta Engineering Resilience: Lessons from Chaos Engineering Journey di Amazon Search.

Obiettivi basati sulle metriche

È possibile stabilire obiettivi basati su metriche quantitative, ad esempio un punteggio di resilienza calcolato assegnando punti a servizi che adottano best practice comprovate in materia di resilienza. È quindi possibile utilizzare particolari esperimenti di caos per determinare il punteggio di resilienza. Questo punteggio può servire come misura per i team per monitorare i progressi compiuti nella mitigazione dei rischi di disponibilità noti e nell'implementazione delle misure di resilienza consigliate. Tuttavia, è fondamentale interpretare tali punteggi con cautela ed evitare di enfatizzare eccessivamente una singola metrica a scapito di obiettivi di resilienza più ampi. Per un esempio, vedi Comprendere i punteggi di resilienza.

Obiettivi di conformità normativa

Il settore dei servizi finanziari si è dimostrato all'avanguardia nell'adozione dell'ingegneria del caos, guidato principalmente da severi requisiti normativi che impongono solide capacità di resilienza. Le normative richiederanno che gli istituti finanziari identifichino, testino e risolvano in modo proattivo le vulnerabilità nei loro sistemi e processi critici. Queste normative includono quanto segue:

- Il documento interagenziale sulle buone pratiche per rafforzare la resilienza operativa pubblicato dalle agenzie federali statunitensi
- Le linee guida della Banca centrale europea sulla resilienza operativa
- La proposta della Commissione europea per una legge sulla resilienza operativa digitale (DORA)

Se la tua organizzazione è un istituto finanziario, rispetta queste normative fissando obiettivi espliciti per dimostrare la resilienza operativa attraverso strategie complete di test e convalida. Ad esempio, vedi London Stock Exchange Group utilizza l'ingegneria del caos per migliorare la resilienza. AWS

Appendice B – Misure quantitative e qualitative

Questa sezione descrive le metriche quantitative per tenere traccia dei miglioramenti operativi e le misure qualitative per valutare i risultati organizzativi più ampi derivanti dalle pratiche di ingegneria del caos.

Misure quantitative

Le seguenti misure quantitative forniscono un quadro per il monitoraggio delle metriche chiave in grado di dimostrare gli incidenti diretti e i miglioramenti operativi raggiunti attraverso le pratiche di ingegneria del caos:

- Incidenti:
  - Frequenza degli incidenti – Tieni traccia del numero di incidenti all'interno di un quadro di classificazione degli incidenti e li classifica in base alla loro criticità (critica, grave, minore) per un periodo di tempo. Per ulteriori informazioni sul quadro di classificazione degli incidenti, vedere l'Appendice C.
  - Tempi di inattività e degrado – Misura la durata totale del downtime o del degrado del servizio per ogni classificazione degli incidenti.
  - Metriche di risposta agli incidenti – Per comprendere gli incidenti, misura il tempo di rilevamento, il tempo di identificazione, il tempo di mitigazione, il tempo di ripristino, il tempo di intensificazione e altre metriche correlate per ogni classificazione degli incidenti.
  - Incidenti con impatto sui clienti – Tieni traccia del numero di incidenti che hanno un impatto sui clienti o della percentuale di incidenti che erano stati risolti prima dell'impatto sui clienti.
  - Modifiche al runbook – Tieni traccia del numero di aggiornamenti o revisioni del runbook derivanti dalle informazioni acquisite attraverso esperimenti di caos. Un runbook fornisce istruzioni dettagliate per eseguire una particolare operazione o procedura per il ripristino da un particolare tipo di incidente.
- Costi:
  - Costi dell'infrastruttura – Raccogli dati sui costi dell'infrastruttura, comprese le risorse di cloud computing e le misure di ridondanza richieste dalle azioni intraprese per migliorare la resilienza.
  - Impatto sul cliente – Misura gli impatti sull'esperienza del cliente, i tassi di abbandono e le perdite di entrate associate a guasti del sistema o tempi di inattività.

    - Produttività del personale – Tieni traccia del tempo impiegato dai team tecnici e operativi per la risposta agli incidenti, la lotta antincendio, la stesura di autopsie e altre attività reattive relative ai guasti del sistema.
- Miglioramenti continui del sistema – Conta il numero di miglioramenti dei processi, modifiche all'architettura o meccanismi di ripristino automatizzati implementati come risultato diretto delle informazioni ottenute da esperimenti sul caos.
- Conformità – Tieni traccia dei costi e lavora per soddisfare i requisiti normativi o gli standard di settore relativi alla resilienza operativa.
- Adozione – Monitora il tasso di adozione delle pratiche legate al caos in tutta l'organizzazione.
- Soddisfazione del cliente – Misura i cambiamenti nelle metriche di soddisfazione dei clienti per valutare in che modo una maggiore affidabilità del sistema influisce sull'azienda.

Misure qualitative

Le seguenti misure qualitative forniscono un quadro per tracciare i più ampi risultati organizzativi raggiunti attraverso le pratiche di ingegneria del caos:

- Fiducia e preparazione dei dipendenti:
    - Sondaggi periodici tra i team per misurare il loro livello di fiducia nella gestione degli incidenti del mondo reale e la loro predisposizione percepita alle interruzioni di chiamata.
    - Tieni traccia della percentuale di tecnici a chiamata che hanno partecipato a esperimenti sul caos nell'ambito della loro formazione.
- Cambiamento culturale:
    - Valuta il grado in cui una mentalità di resilienza ha permeato l'organizzazione attraverso sondaggi, sessioni di feedback o audit.
    - Tieni traccia del numero di team che difendono e difendono attivamente le pratiche di ingegneria del caos.
- Collaborazione interfunzionale e condivisione delle conoscenze:
    - Tieni traccia della frequenza e della partecipazione alle sessioni o ai workshop di condivisione delle conoscenze tra team relativi all'apprendimento dell'ingegneria del caos.
    - Tieni traccia del numero di iniziative congiunte di ingegneria del caos che coinvolgono più team o reparti.
- Efficacia della formazione:

  - Valuta l'efficacia dei programmi di formazione sull'ingegneria del caos conducendo sondaggi o valutazioni post-formazione.
  - Tieni traccia del numero di ingegneri che partecipano ai programmi di formazione sull'ingegneria del caos e leggi le autopsie.
- Attrazione e fidelizzazione dei talenti:
  - Valuta se il programma di ingegneria del caos aiuta ad attrarre e fidelizzare i migliori talenti ingegneristici riducendo il tempo e gli sforzi spesi per risolvere le interruzioni.
- Reputazione del marchio:
  - Tieni traccia di eventuali cambiamenti nella percezione o nella reputazione del marchio correlati all'impegno dimostrato dell'organizzazione per la resilienza operativa.
- Vantaggio competitivo:
  - Tieni traccia del vantaggio competitivo rispetto ai concorrenti del settore in termini di disponibilità del sistema.

Appendice C – Classificazione degli incidenti

Il monitoraggio degli incidenti all'interno di un framework di classificazione è fondamentale perché il framework fornisce una visione olistica dei tipi di guasto e dei problemi che hanno un impatto sul sistema. Se l'organizzazione tiene traccia degli incidenti solo all'interno di un'unica categoria, ad esempio i guasti dell'infrastruttura, potrebbe perdere informazioni e opportunità di miglioramento in altre aree. Monitorando gli incidenti su più classi, si ottiene una migliore comprensione della vasta gamma di esperimenti sul caos da condurre. Questa prospettiva aiuta a identificare potenziali punti ciechi e supporta l'espansione dell'ambito ingegneristico, il che porta a un sistema più resiliente e tollerante ai guasti.

Il framework di classificazione degli incidenti suggerito è progettato per aiutare a classificare gli incidenti in base alla loro natura e al potenziale impatto. Utilizza una classificazione di alto livello che raggruppa gli incidenti in otto categorie principali:

- Problemi di distribuzione:
  - Implementazioni non riuscite
  - Errori di rollback
  - Problemi di configurazione durante la distribuzione
- Bug e regressioni del software:
  - Bug funzionali
  - Problemi di integrazione
  - Problemi di prestazioni
  - Problemi relativi alle quote
  - Problemi relativi al meccanismo di resilienza (nuovi tentativi, timeout)
  - Problemi di integrità dei dati
- Problemi relativi ai test:
  - Test mancanti
  - Test inefficaci
  - Test Flaky
- Guasti dell'infrastruttura:
  - Guasti hardware (server, dispositivi di rete, storage)
  - Problemi di scalabilità

    - Errori di dipendenza (servizi di terze parti,) APIs
    - Problemi di connettività di rete
- Problemi operativi:
    - Errori umani (configurazione errata, modifiche accidentali)
    - Monitoraggio e segnalazione degli errori
    - Problemi di pianificazione della capacità
    - Errori di backup e ripristino
- Incidenti di sicurezza:
    - Tentativi di accesso non autorizzati
    - Violazioni dei dati
    - Attacchi Denial of Service (DoS)
- Interruzioni del servizio di terze parti:
    - Interruzioni dei provider di servizi cloud
    - Guasti DNS
    - Interruzioni esterne delle API e dei servizi
- Fattori ambientali:
    - Disastri naturali (terremoti, incendi, inondazioni, interruzioni di corrente)
    - Problemi legati alle condizioni meteorologiche

Questo è un esempio non conclusivo di framework di classificazione che puoi personalizzare in base alle tue esigenze e alla tua organizzazione specifiche. Consigliamo di rivedere e aggiornare periodicamente il framework di classificazione man mano che il sistema si evolve o emergono nuovi tipi di incidenti.

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	—	28 gennaio 2025

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.