Implementazione dei controlli di sicurezza su AWS

AWS Guida prescrittiva

AWS Guida prescrittiva: Implementazione dei controlli di sicurezza su AWS

Table of Contents

Implementazione dei controlli di sicurezza in AWS

Iqbal Umair, Gurpreet Kaur Cheema, Wasim Hossain, Joseph Nguyen, San Brar e Lucia Vanta, Amazon Web Services (AWS)

Dicembre 2023 (cronologia dei documenti)

La sicurezza è un tema cruciale per ogni azienda e rappresenta un pilastro fondamentale del Framework AWS Well-Architected. Tuttavia, è spesso complesso gestire le considerazioni relative alla sicurezza e creare una strategia olistica di test e correzione della sicurezza automatizzata per i propri ambienti cloud. Utilizzando gli strumenti e i Servizi AWS, come AWS Config, Amazon GuardDuty e AWS CloudFormation, puoi creare una strategia di approccio ai test di sicurezza e integrarla negli ambienti Cloud AWS.

I controlli di sicurezza sono guardrail tecnici o amministrativi che impediscono, rilevano o riducono la capacità di un autore di minacce di sfruttare una vulnerabilità di sicurezza, contribuendo così a soddisfare le policy e gli standard di sicurezza dell'azienda. Sono progettati per proteggere la riservatezza, l'integrità e la disponibilità di risorse e dati. Di seguito sono riportati alcuni esempi di controlli di sicurezza:

- Implementazione dell'autenticazione a più fattori per gli utenti che devono accedere a un'applicazione
- Operazioni di registrazione, monitoraggio e interrogazione allo scopo di eseguire controlli in tempo reale in merito all'attività dell'account
- Crittografia dei dati sensibili
- Archiviazione dei log in base alla policy di conservazione dell'azienda

Esistono quattro tipi di controlli di sicurezza: preventivo, proattivo, di rilevamento e reattivo. Questa guida descrive ognuno di essi in modo dettagliato e illustra il modo in cui implementare e automatizzare questi controlli nel Cloud AWS. Questa guida consente di implementare i controlli di sicurezza in modo continuo e proattivo.

Destinatari principali

Questa guida è destinata agli architect e agli ingegneri della sicurezza responsabili dell'implementazione dei controlli di sicurezza nel Cloud AWS. Se l'azienda non ha ancora stabilito

le policy di sicurezza, gli obiettivi di controllo o gli standard, come descritto nella sezione Controlli di sicurezza nel framework di governance, ti consigliamo di completare queste attività di governance prima di procedere con questa guida.

Obiettivi aziendali specifici

Le aziende utilizzano i controlli di sicurezza per mitigare i rischi o agire come contromisure per i propri sistemi IT. I controlli definiscono la baseline dei requisiti per soddisfare i principali obiettivi di sicurezza di un programma IT e della relativa strategia. La presenza di controlli migliora la posizione di sicurezza di un'azienda, proteggendo la riservatezza, l'integrità e la disponibilità dei dati e delle risorse IT. Senza controlli, sarebbe difficile conoscere l'area in cui investire per stabilire una baseline di sicurezza.

I controlli di sicurezza possono essere utilizzati per affrontare una varietà di scenari. Gli esempi includono il rispetto dei requisiti derivanti dalla valutazione del rischio, il raggiungimento degli standard di settore o la conformità alle normative. Con l'applicazione dei controlli di sicurezza, puoi dimostrare di aver calcolato il rischio di un sistema, determinato il livello di protezione necessario e implementato le soluzioni in modo proattivo. È possibile stabilire i controlli di sicurezza anche in base ad altri fattori, come l'attività, il settore e la posizione geografica.

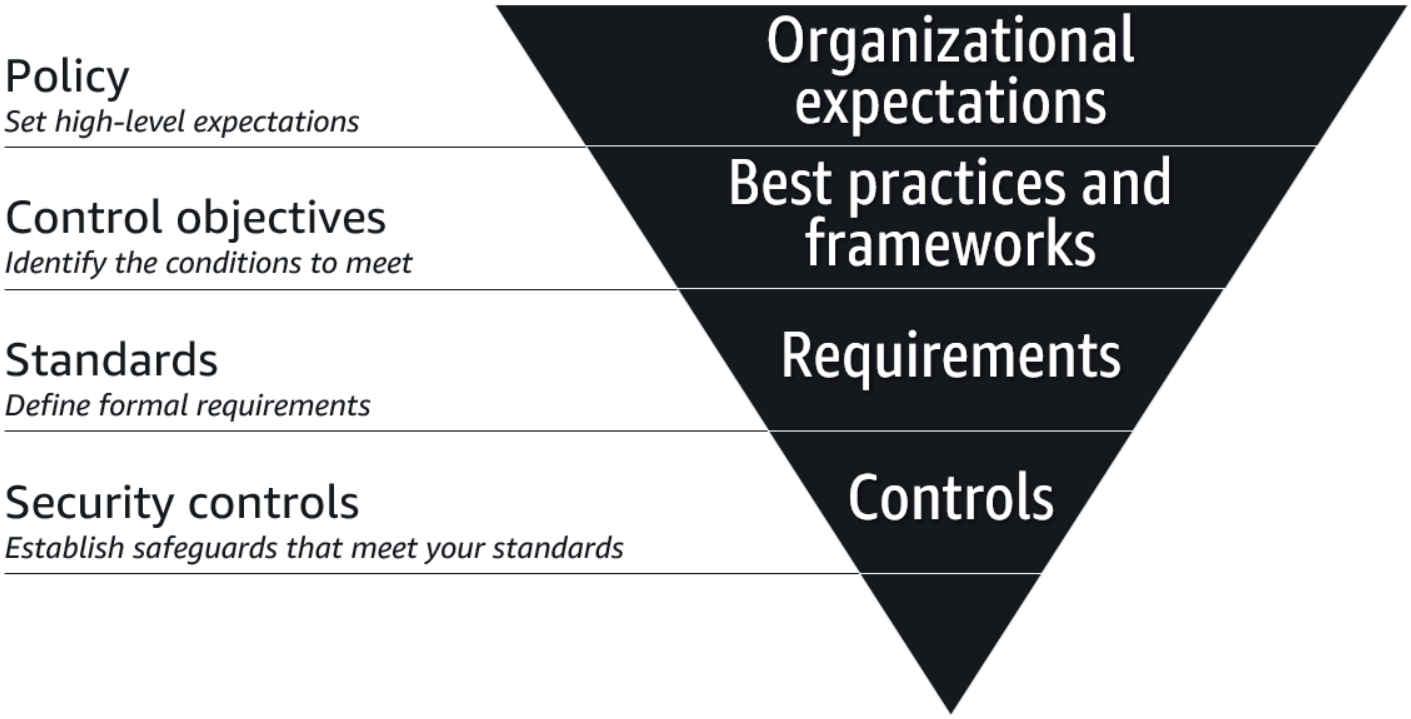
Di seguito sono riportati i casi d'uso più comuni per l'implementazione dei controlli di sicurezza:

- La valutazione di sicurezza di un'applicazione ha rilevato la necessità di controlli di accesso in base alla sensibilità dei dati elaborati.
- È necessario rispettare gli standard di sicurezza, come PCI DSS (Payment Card Industry Data Security Standard, standard di sicurezza dei dati dell'industria delle carte di pagamento), HIPAA (Health Insurance Portability and Accountability Act, legge sulla portabilità e responsabilità delle polizze di assicurazione sanitaria) o NIST (National Institute of Standards and Technology).
- È necessario proteggere le informazioni sensibili per le transazioni commerciali.
- L'azienda si è espansa in un'area geografica che richiede controlli di sicurezza, ad esempio una regione che richiede la conformità al GDPR (General Data Protection Regulation, regolamento generale sulla protezione dei dati).

La lettura di questa sezione dovrebbe consentirti di acquisire familiarità con i quattro tipi di controlli di sicurezza, comprendere il modo in cui fanno parte del framework di governance della sicurezza e iniziare a implementare e automatizzare i controlli di sicurezza nel Cloud AWS.

Controlli di sicurezza nel framework di governance

È importante pianificare a partire da un livello di base. Come si inizia? La figura seguente mostra il modo in cui puoi creare una strategia di governance della sicurezza basata su policy, obiettivi di controllo, standard e controlli di sicurezza.



Di seguito sono riportati i componenti gerarchici di una strategia di governance della sicurezza:

- Policy: una policy è la base di qualsiasi strategia di governance della sicurezza informatica. Si tratta di un documento che indica le aspettative dell'azienda, ad esempio gli obblighi statutari, normativi o contrattuali da rispettare. Le policy possono variare in base al settore e alla regione.
- Obiettivi di controllo: gli obiettivi di controllo, ad esempio le best practice riconosciute dal settore, consentono di soddisfare l'intento di una policy. Per quanto riguarda il cloud computing, molte aziende adottano Cloud Controls Matrix (CCM) (sito Web di Cloud Security Alliance), ossia un framework di obiettivi di controllo della sicurezza informatica.
- Standard: gli standard sono requisiti formalmente stabiliti che soddisfano un obiettivo di controllo. Possono includere processi, operazioni o configurazioni e sono quantificabili in modo da poter misurare le prestazioni rispetto alla normale operatività.
- Controlli di sicurezza: i controlli di sicurezza sono meccanismi tecnici o amministrativi messi in atto per implementare gli standard. Tutti i controlli di sicurezza vengono mappati agli standard, ma

non viceversa. La verifica dei controlli di sicurezza è finalizzata a monitorare e misurare l'effettivo rispetto degli standard definiti.

Questa guida descrive come progettare e implementare i tipi più comuni di controlli di sicurezza nel Cloud AWS.

Tipi di controlli di sicurezza

Esistono quattro tipi principali di controlli di sicurezza:

- Controlli preventivi: progettati per evitare il verificarsi di un evento.
- Controlli proattivi: progettati per impedire la creazione di risorse non conformi.
- Controlli di rilevamento: progettati per rilevare, registrare e avvisare dopo che si è verificato un evento.
- Controlli reattivi: progettati per correggere gli eventi avversi o le deviazioni dalla baseline di sicurezza.

Una strategia di sicurezza efficace include tutti e quattro i tipi di controlli di sicurezza. Sebbene i controlli preventivi rappresentino la prima linea di difesa per evitare accessi non autorizzati o modifiche indesiderate alla rete, è importante assicurarsi di stabilire controlli di rilevamento e reattivi in modo da sapere quando si verifica un evento e poter intraprendere azioni immediate e appropriate per porvi rimedio. L'utilizzo di controlli proattivi aggiunge un ulteriore livello di sicurezza perché integra i controlli preventivi, generalmente di natura più rigorosa.

Le sezioni seguenti descrivono ogni tipo di controllo in modo più dettagliato. Vengono illustrati gli obiettivi, il processo di implementazione, i casi d'uso, le considerazioni tecnologiche e i risultati specifici di ogni tipo di controllo.

Controlli preventivi

I controlli preventivi sono controlli di sicurezza progettati per impedire il verificarsi di un evento. Questi guardrail rappresentano la prima linea di difesa per impedire accessi non autorizzati o modifiche indesiderate alla rete. Un esempio di controllo preventivo è un ruolo AWS Identity and Access Management (IAM) con accesso in sola lettura perché aiuta a prevenire azioni di scrittura involontarie da parte di utenti non autorizzati.

Leggi quanto segue su questo tipo di controllo:

- Obiettivi
- Processo
- Casi d'uso
- Tecnologia

- Risultati aziendali

Obiettivi

Lo scopo principale dei controlli preventivi è ridurre al minimo o evitare la probabilità che si verifichi un evento minaccioso. Il controllo deve favorire la prevenzione di accessi non autorizzati al sistema e impedire che le modifiche involontarie influiscano sul sistema. Gli obiettivi dei controlli preventivi sono i seguenti:

- Segregazione delle attività. I controlli preventivi possono stabilire confini logici che limitano i privilegi, consentendo l'esecuzione di attività specifiche solo in account o ambienti designati. Esempi includono:
  - Segmentare i carichi di lavoro in diversi account per servizi specifici
  - Separare e contabilizzare in ambienti di produzione, sviluppo e test isolati
  - Delegare l'accesso e le responsabilità a più entità per lo svolgimento di funzioni specifiche, ad esempio utilizzando ruoli IAM o ruoli presunti per consentire l'esecuzione di determinate azioni solo a funzioni di processo specifiche
- Controllo degli accessi. I controlli preventivi possono concedere o negare in modo coerente l'accesso a risorse e dati nell'ambiente. Esempi includono:
  - Impedire agli utenti di superare le autorizzazioni previste, una tecnica nota come escalation dei privilegi
  - Limitare l'accesso alle applicazioni e ai dati solo agli utenti e ai servizi autorizzati
  - Un ridotto gruppo di amministratori
  - Evitare l'uso delle credenziali dell'utente root
- Applicazione. I controlli preventivi possono aiutare l'azienda a rispettare le policy, le linee guida e gli standard aziendali. Esempi includono:
  - Bloccare le configurazioni che fungono da baseline di sicurezza minima
  - Implementare misure di sicurezza aggiuntive, come l'autenticazione a più fattori
  - Evitare attività e operazioni non standard eseguite da ruoli non approvati

Processo

La mappatura dei controlli preventivi è il processo di mappatura dei controlli ai requisiti e alle policy di utilizzo per implementare tali controlli mediante restrizioni, disabilitazioni o blocchi. Quando si

mappano i controlli, bisogna considerare l'effetto proattivo che hanno sull'ambiente, sulle risorse e sugli utenti. Di seguito sono riportate le best practice per la mappatura dei controlli:

- I controlli rigorosi che non consentono un'attività devono essere mappati agli ambienti di produzione in cui l'operazione richiede processi di revisione, approvazione e modifica.
- Gli ambienti di sviluppo o indipendenti possono avere meno controlli preventivi al fine di fornire l'agilità necessaria per la creazione e il test.
- I controlli preventivi vengono stabiliti in base alla classificazione dei dati, al livello di rischio di una risorsa e alla policy di gestione del rischio.
- Eseguire la mappatura ai framework esistenti come prova della conformità a standard e regolamenti.
- Implementare i controlli preventivi in base a posizione geografica, ambiente, account, reti, utenti, ruoli o risorse.

Casi d'uso

Gestione dei dati

Viene creato un ruolo in grado di accedere a tutti i dati di un account. Se sono presenti dati sensibili e crittografati, i privilegi troppo permissivi potrebbero rappresentare un rischio, a seconda degli utenti o dei gruppi che possono assumere il ruolo. Utilizzando una policy chiave in AWS Key Management Service (AWS KMS), puoi controllare chi ha accesso alla chiave e può decrittografare i dati.

Escalation dei privilegi

Se le autorizzazioni amministrative e di scrittura vengono assegnate in modo troppo ampio, un utente può aggirare i limiti delle autorizzazioni previste e concedersi privilegi aggiuntivi. L'utente che crea e gestisce un ruolo può assegnare un limite delle autorizzazioni che definisce i privilegi massimi consentiti per tale ruolo.

Blocco del carico di lavoro

Se la tua azienda non ha la necessità prevedibile di utilizzare servizi specifici, abilita una politica di controllo dei servizi che limiti i servizi che possono funzionare negli account dei membri di un'organizzazione o limiti i servizi in base a. Regione AWS Se un autore di minacce riesce a compromettere e ad accedere a un account dell'organizzazione, questo controllo preventivo può

ridurre la portata dell'impatto. Per ulteriori informazioni sul tagging, consulta Policy di controllo dei serviziin questa guida.

Impatto su altre applicazioni

I controlli preventivi possono imporre l'uso di determinati servizi e funzionalità, come IAM, crittografia e registrazione, per soddisfare i requisiti di sicurezza delle applicazioni. Puoi inoltre utilizzare tali controlli per proteggerti dalle vulnerabilità, limitando le operazioni che un autore di minacce può sfruttare a causa di errori involontari o di una configurazione errata.

Tecnologia

Policy di controllo dei servizi

Nel AWS Organizations, le politiche di controllo dei servizi (SCP) definiscono le autorizzazioni massime disponibili per gli account dei membri di un'organizzazione. Queste policy consentono agli account di rispettare le linee guida per il controllo degli accessi dell'organizzazione. Durante la progettazione delle policy di controllo dei servizi per l'organizzazione, tieni presente quanto segue:

- Gli SCP sono controlli preventivi perché definiscono e applicano le autorizzazioni massime consentite per i ruoli e gli utenti IAM negli account dei membri dell'organizzazione.
- Gli SCP influiscono solo sui ruoli e sugli utenti IAM negli account dei membri dell'organizzazione. non nell'account di gestione.

Puoi rendere più granulare una policy di controllo dei servizi definendo le autorizzazioni massime per ogni Regione AWS.

Limiti delle autorizzazioni IAM

In AWS Identity and Access Management (IAM), un limite di autorizzazioni viene utilizzato per impostare le autorizzazioni massime che una policy basata sull'identità può concedere a un'entità IAM (utenti o ruoli). Il limite delle autorizzazioni di un'entità consente di eseguire solo le operazioni consentite dalle policy basate sull'identità e dai relativi limiti delle autorizzazioni. Per quanto riguarda l'utilizzo dei limiti delle autorizzazioni, tieni presente quanto segue:

- È possibile utilizzare una policy gestita o una policy AWS gestita dal cliente per impostare il limite per un'entità IAM.
- Il limite delle autorizzazioni non concedere l'accesso di per sé. La policy per il limite delle autorizzazioni riduce le autorizzazioni concesse all'entità IAM.

Risultati aziendali

Risparmi di tempo

- L'aggiunta di un'automazione dopo aver impostato i controlli preventivi consente di ridurre la necessità di intervento manuale e la frequenza degli errori.
- L'utilizzo dei limiti delle autorizzazioni come controllo preventivo aiuta i team di sicurezza e IAM a concentrarsi su attività critiche, come la governance e il supporto.

Conformità alle normative

- È possibile che le aziende debbano rispettare delle normative interne o di settore, come restrizioni regionali, limitazioni relative a utenti e ruoli o restrizioni del servizio. Le SCP possono aiutarti a mantenere la conformità ed evitare sanzioni legate alle violazioni.

Riduzione del rischio

- Con la crescita, aumenta il numero di richieste per creare e gestire nuovi ruoli e policy. Diventa più difficile comprendere il contesto di ciò che è necessario per creare manualmente le autorizzazioni per ciascuna applicazione. L'istituzione di controlli preventivi funge da baseline e impedisce agli utenti di eseguire operazioni indesiderate, anche nel caso in cui l'accesso è stato concesso in modo non intenzionale.
- L'applicazione di controlli preventivi alle policy di accesso offre un ulteriore livello di protezione dei dati e delle risorse.

Controlli proattivi

I controlli proattivi sono controlli di sicurezza progettati per impedire la creazione di risorse non conformi. Questi controlli possono ridurre il numero di eventi di sicurezza gestiti da controlli reattivi e di rilevamento. Questi controlli assicurano che le risorse distribuite siano conformi prima di essere distribuite; pertanto, non vi è alcun evento di rilevamento che richieda una risposta o una correzione.

Ad esempio, puoi applicare un controllo di rilevamento che indichi il momento in cui un bucket Amazon Simple Storage Service (Amazon S3) diventa accessibile al pubblico e avvisare l'utente. Potresti anche disporre di un controllo reattivo per correggere il problema. Oltre a questi due controlli, puoi aggiungere un altro livello di protezione aggiungendo un controllo proattivo. In questo modo

AWS CloudFormation, il controllo proattivo può impedire la creazione di aggiornamenti di qualsiasi bucket S3 con accesso pubblico abilitato. I responsabili delle minacce potrebbero comunque aggirare questo controllo e distribuire o modificare risorse esterne a. CloudFormation In questo caso, i controlli di rilevamento e reattivi risolverebbero l'evento di sicurezza.

Leggi quanto segue su questo tipo di controllo:

- Obiettivi
- Processo
- Casi d'uso
- Tecnologia
- Risultati aziendali

Obiettivi

- I controlli proattivi consentono di migliorare i processi operativi di sicurezza e di qualità.
- I controlli proattivi possono aiutarti a rispettare policy, standard e obblighi normativi o di conformità di sicurezza.
- I controlli proattivi possono impedire la creazione di risorse non conformi.
- I controlli proattivi possono ridurre il numero dei problemi di sicurezza.
- I controlli proattivi forniscono un altro livello di protezione contro gli autori di minacce che aggirano i controlli preventivi e tentano di implementare risorse non conformi.
- Con i controlli preventivi, di rilevamento e reattivi, i controlli proattivi possono aiutarti a risolvere potenziali incidenti di sicurezza.

Processo

I controlli proattivi completano i controlli preventivi. I controlli proattivi riducono i rischi per la sicurezza dell'organizzazione e impongono l'implementazione di risorse conformi. Questi controlli valutano la conformità delle risorse prima che le risorse vengano create o aggiornate. I controlli proattivi vengono generalmente implementati utilizzando hook. CloudFormation Se la risorsa non supera la convalida del controllo proattivo, puoi scegliere di rinunciare all'implementazione della risorsa o di presentare un messaggio di avviso. Di seguito, sono riportati alcuni suggerimenti e best practice per la creazione di controlli proattivi:

- Assicurati che i controlli proattivi siano mappati ai requisiti di conformità della tua organizzazione.

- Assicurati che i controlli proattivi seguano le best pratice di sicurezza per il servizio associato.
- Utilizza CloudFormation StackSets o un'altra soluzione per implementare controlli proattivi su più account. Regioni AWS
- Assicurati che il messaggio di avviso o di errore associato a un controllo proattivo sia esplicito e chiaro. Questo aiuta gli sviluppatori a capire il motivo per cui la risorsa non ha superato la valutazione.
- Quando crei nuovi controlli proattivi, inizia in modalità osservazione. Ciò significa che invii un messaggio di avviso invece di fallire l'implementazione delle risorse. Questo ti aiuta a comprendere l'impatto del controllo proattivo.
- Abilita la registrazione in Amazon CloudWatch Logs per controlli proattivi.
- Se devi monitorare l'invocazione di un controllo proattivo specifico, utilizza una EventBridge regola Amazon e iscriviti agli eventi di invocazione per l'hook. CloudFormation

Casi d'uso

- Impedisci l'implementazione di risorse non conformi
- Requisiti sempre soddisfatti
- Migliora la qualità del codice imponendo la risoluzione di un problema di sicurezza prima dell'implementazione
- Riduci i tempi di inattività operativi associati alla risoluzione dei problemi di sicurezza dopo l'implementazione

Tecnologia

CloudFormation ganci

AWS CloudFormationti aiuta a configurare AWS le risorse, fornirle in modo rapido e coerente e gestirle durante tutto il loro ciclo di vita in tutte le regioni Account AWS . CloudFormation gli hook valutano in modo proattivo la configurazione delle CloudFormation risorse prima che vengano distribuite. Se vengono trovate risorse non conformi, restituisce uno stato di errore. In base alla modalità di errore dell'hook, CloudFormation può fallire l'operazione o presentare un avviso che consente all'utente di continuare con la distribuzione. È possibile utilizzare gli hook disponibili oppure svilupparne di propri.

AWS Control Tower

AWS Control Towerti aiuta a configurare e gestire un ambiente AWS multi-account, seguendo le migliori pratiche prescrittive. AWS Control Tower offre controlli proattivi preconfigurati che puoi abilitare nella tua landing zone. Se la tua landing zone è configurata utilizzando AWS Control Tower, puoi utilizzare questi controlli proattivi opzionali come punto di partenza per la tua organizzazione. È possibile creare controlli proattivi aggiuntivi e personalizzati in base alle esigenze CloudFormation .

Risultati aziendali

Meno errori e sforzi umani

I controlli proattivi riducono il rischio di errori umani che portano all'implementazione di risorse non conformi. Inoltre, riducono l'impegno umano nelle fasi successive del ciclo di sviluppo: inducono gli sviluppatori a prendere in considerazione la sicurezza delle risorse prima dell'implementazione. Ciò applica la prassi shift a sinistra alla creazione di risorse sicure perché impone la conformità nelle fasi iniziali del ciclo di vita dello sviluppo.

Riduzione dei costi

In genere, è più costoso risolvere un problema di sicurezza dopo l'implementazione. L'identificazione e la risoluzione dei problemi nelle fasi iniziali del ciclo di sviluppo riducono i costi di sviluppo.

Risparmi di tempo

Poiché i controlli proattivi impediscono l'implementazione di risorse non conformi, riducono la quantità di tempo dedicata alla valutazione e alla risoluzione dei problemi di sicurezza. Inoltre, riguardano il numero di rilevamenti di sicurezza, che i controlli investigativi identificheranno più avanti nel ciclo di sviluppo.

Conformità alle normative

Se l'organizzazione deve rispettare le normative interne o di settore, i controlli proattivi possono aiutarti a mantenere la conformità ed evitare sanzioni legate alle violazioni.

Riduzione del rischio

I controlli proattivi aiutano gli sviluppatori a distribuire risorse conformi e costruite in modo più sicuro, cosi da ridurre rischi per la sicurezza dell'organizzazione.

Controlli di rilevamento

I controlli di rilevamento sono progettati per rilevare, registrare e avvisare dopo che si è verificato un evento. Costituiscono pertanto una parte fondamentale dei framework di governance. Questi guardrail rappresentano una seconda linea di difesa, in quanto segnalano all'utente gli eventuali problemi di sicurezza che hanno eluso i controlli preventivi.

Ad esempio, puoi applicare un controllo di rilevamento per identificare il momento in cui un bucket Amazon Simple Storage Service (Amazon S3) diventa accessibile al pubblico e avvisare l'utente. Anche se potresti disporre di controlli preventivi che disabilitano l'accesso pubblico ai bucket S3 a livello di account e di conseguenza l'accesso tramite le SCP, un autore di minacce potrebbe aggirare questi controlli preventivi accedendo come utente amministrativo. In queste situazioni, un controllo di rilevamento può segnalare l'errata configurazione e la potenziale minaccia.

Leggi quanto segue su questo tipo di controllo:

- Obiettivi
- Processo
- Casi d'uso
- Tecnologia
- Risultati aziendali

Obiettivi

- I controlli di rilevamento consentono di migliorare i processi operativi di sicurezza e i processi di qualità.
- I controlli di rilevamento consentono di soddisfare i requisiti normativi, legali o di conformità.
- I controlli di rilevamento offrono ai team addetti alle operazioni di sicurezza la visibilità necessaria per rispondere ai problemi di sicurezza, tra cui le minacce avanzate che eludono i controlli preventivi.
- I controlli di rilevamento consentono di identificare la risposta appropriata ai problemi di sicurezza e alle potenziali minacce.

Processo

L'implementazione dei controlli di rilevamento avviene in due fasi. Innanzitutto, configuri il sistema per registrare gli eventi e gli stati delle risorse in una posizione centralizzata, come Amazon CloudWatch Logs. Dopo aver configurato la registrazione centralizzata, analizza i log per identificare eventuali anomalie che potrebbero indicare una minaccia. Ogni analisi è un controllo mappato in base ai requisiti e alle policy originali. Ad esempio, puoi creare un controllo di rilevamento in grado di cercare uno schema specifico nei log e generare un avviso in caso di corrispondenza. I controlli di rilevamento vengono utilizzati dai team di sicurezza per migliorare la visibilità complessiva delle minacce e dei rischi a cui il sistema potrebbe essere esposto.

Casi d'uso

Rilevamento di comportamenti sospetti

I controlli di rilevamento consentono di identificare qualsiasi attività anomala, come la compromissione delle credenziali utente con privilegi oppure l'accesso o l'esfiltrazione di dati sensibili. Questi controlli sono importanti fattori reattivi che possono aiutare l'azienda a identificare e comprendere la portata delle attività anomale.

Rilevamento delle frodi

Questi controlli consentono di rilevare e identificare una minaccia all'interno dell'azienda, ad esempio un utente che elude le policy ed esegue transazioni non autorizzate.

Conformità

I controlli di rilevamento consentono di soddisfare i requisiti di conformità, come il PCI DSS (Payment Card Industry Data Security Standard, standard di sicurezza dei dati dell'industria delle carte di pagamento) e possono contribuire a prevenire il furto di identità. Questi controlli possono scoprire e proteggere le informazioni sensibili soggette a conformità normativa, come le informazioni di identificazione personale.

Analisi automatica

I controlli di rilevamento possono analizzare automaticamente i log al fine di rilevare anomalie e altri indicatori di attività non autorizzate.

Puoi analizzare automaticamente i log provenienti da diverse origini, come i log AWS CloudTrail , i log di flusso VPC e i log del sistema dei nomi di dominio (DNS), per identificare attività

potenzialmente dannose. Per semplificare l'organizzazione, aggrega gli avvisi o i risultati di sicurezza da più postazioni Servizi AWS a una posizione centralizzata.

Tecnologia

Un controllo di rilevamento comune consiste nell'implementazione di uno o più servizi di monitoraggio, in grado di analizzare le origini dati, come i log, per identificare le minacce alla sicurezza. In Cloud AWS, puoi analizzare fonti come AWS CloudTrail log, log di accesso di Amazon S3 e log di flusso di Amazon Virtual Private Cloud per rilevare attività insolite. AWS i servizi di sicurezza, come Amazon GuardDuty, Amazon Detective e Amazon Macie AWS Security Hub, dispongono di funzionalità di monitoraggio integrate.

GuardDuty e Security Hub

Amazon GuardDuty utilizza tecniche di intelligence sulle minacce, apprendimento automatico e rilevamento delle anomalie per monitorare continuamente le fonti di registro alla ricerca di attività dannose o non autorizzate. La dashboard fornisce informazioni in tempo reale sullo stato di salute dei tuoi carichi di lavoro e dei tuoi carichi di lavoro. Account AWS Puoi integrarti GuardDuty con AWS Security Hubun servizio di gestione delle posture di sicurezza nel cloud che verifica l'aderenza alle migliori pratiche, aggrega gli avvisi e consente la correzione automatica. GuardDuty invia i risultati a Security Hub per centralizzare le informazioni. Puoi integrare ulteriormente Security Hub con soluzioni di gestione delle informazioni e degli eventi di sicurezza (SIEM) per estendere le funzionalità di monitoraggio e avviso per l'organizzazione.

Macie

Amazon Macie è un servizio di sicurezza e privacy dei dati completamente gestito che utilizza il machine learning e la corrispondenza di pattern per individuare e proteggere i dati sensibili in AWS. Di seguito sono riportati alcuni controlli di rilevamento e alcune funzionalità disponibili in Macie:

- Macie ispeziona l'inventario dei bucket e tutti gli oggetti archiviati in Amazon S3. Queste informazioni possono essere presentate in un'unica dashboard, offrendo maggiore visibilità e contribuendo a valutare la sicurezza dei bucket.
- Per scoprire i dati sensibili, Macie utilizza identificatori di dati gestiti integrati e supporta inoltre identificatori di dati personalizzati.
- Macie si integra nativamente con altri strumenti. Servizi AWS Ad esempio, Macie emette i risultati come EventBridge eventi Amazon, che vengono inviati automaticamente a Security Hub.

Di seguito sono riportate le best practice per configurare i controlli di rilevamento in Macie:

- Abilita Macie su tutti gli account. Utilizzando la funzionalità di gestione delegata, abilita Macie su più account con AWS Organizations.
- Usa Macie per valutare la posizione di sicurezza dei bucket S3 negli account. Ciò consente di offrire maggiore visibilità per quanto riguarda la posizione e l'accesso ai dati, impedendone così la perdita. Per ulteriori informazioni, consulta la pagina Analisi della posizione di sicurezza di Amazon S3 (documentazione di Macie).
- Automatizza il rilevamento di dati sensibili nei bucket S3 mediante l'esecuzione e la pianificazione di processi automatici di elaborazione e individuazione dei dati. In questo modo, i bucket S3 vengono ispezionati alla ricerca di dati sensibili in base a una pianificazione regolare.

AWS Config

AWS Configverifica e registra la conformità delle risorse. AWS AWS Config rileva AWS le risorse esistenti e genera un inventario completo, insieme ai dettagli di configurazione di ciascuna risorsa. In caso di modifiche alla configurazione, registra tali modifiche e invia una notifica. Ciò può aiutarti a rilevare e ripristinare le modifiche non autorizzate apportate all'infrastruttura. È possibile utilizzare regole AWS gestite e creare regole personalizzate.

Di seguito sono riportate le best practice per configurare i controlli di rilevamento in AWS Config:

- AWS Config Abilitalo per ogni account membro dell'organizzazione e per ogni Regione AWS account contenente risorse che desideri proteggere.
- Imposta gli avvisi di Amazon Simple Notification Service (Amazon SNS) per notificare eventuali modifiche alla configurazione.
- Archivia i dati di configurazione in un bucket S3 e analizzali con Amazon Athena.
- Automatizza la correzione delle risorse non conformi tramite Automazione, una funzionalità di AWS Systems Manager.
- Usa EventBridge o Amazon SNS per configurare le notifiche sulle risorse non AWS conformi.

Trusted Advisor

AWS Trusted Advisor può essere utilizzato come servizio per i controlli di rilevamento. Attraverso una serie di controlli, Trusted Advisor identifica le aree in cui è possibile ottimizzare l'infrastruttura, migliorare le prestazioni e la sicurezza o ridurre i costi. Trusted Advisor fornisce consigli basati sulle

AWS migliori pratiche che è possibile seguire per migliorare i servizi e le risorse. I piani Business ed Enterprise Support forniscono l'accesso a tutti i controlli disponibili per i pilastri del AWS Well-Architected Framework.

Di seguito sono riportate le best practice per configurare i controlli di rilevamento in Trusted Advisor:

- Esamina il riepilogo del livello di controllo
- Implementa i consigli specifici delle risorse per gli stati di avviso ed errore.
- Controlla Trusted Advisor frequentemente per esaminare e implementare attivamente i suoi consigli.

Amazon Inspector

Amazon Inspector è un servizio di gestione delle vulnerabilità automatizzato che, dopo essere stato attivato, scansiona continuamente i carichi di lavoro alla ricerca di vulnerabilità software ed esposizioni alla rete non intenzionali. Contestualizza gli esiti in un punteggio di rischio che può aiutarti a determinare i passaggi successivi, come la correzione o la conferma dello stato di conformità.

Di seguito sono riportate le best practice per configurare i controlli di rilevamento in Amazon Inspector:

- Abilita Amazon Inspector su tutti gli account e integralo in EventBridge un Security Hub per configurare report e notifiche per le vulnerabilità di sicurezza.
- Assegna priorità alle correzioni e ad altre operazioni in base al punteggio di rischio di Amazon Inspector.

Risultati aziendali

Meno errori e sforzi umani

Puoi sfruttare l'automazione utilizzando l'infrastruttura come codice (IaC). L'automazione dell'implementazione e della configurazione di servizi e strumenti di monitoraggio e correzione riduce il rischio di errori manuali e diminuisce il tempo e l'impegno necessari per dimensionare tali controlli di rilevamento. L'automazione consente di sviluppare i runbook di sicurezza e riduce le operazioni manuali degli analisti della sicurezza. Le revisioni periodiche consentono di ottimizzare gli strumenti di automazione, iterando e migliorando in modo continuo i controlli di rilevamento.

Operazioni appropriate contro potenziali minacce

Per ottenere visibilità è fondamentale acquisire e analizzare gli eventi da log e parametri. In questo modo, gli analisti possono agire in base agli eventi di sicurezza e alle potenziali minacce, proteggendo i carichi di lavoro. La capacità di identificare rapidamente le vulnerabilità esistenti consente agli analisti di intraprendere le azioni appropriate per affrontarle e porvi rimedio.

Migliore risposta agli incidenti e gestione del rilevamento

L'automazione degli strumenti di controllo di rilevamento può aumentare la velocità di individuazione, indagine e ripristino. Le notifiche e gli avvisi automatizzati basati su condizioni definite consentono agli analisti della sicurezza di indagare e rispondere in modo appropriato. Questi fattori reattivi possono aiutarti a identificare e comprendere l'ambito delle attività anomale.

Controlli reattivi

I controlli reattivi sono progettati per correggere gli eventi avversi o le deviazioni dalla baseline di sicurezza. Esempi di controlli reattivi tecnici includono l'applicazione di patch a un sistema, la messa in quarantena di un virus, l'arresto di un processo o il riavvio di un sistema.

Leggi quanto segue su questo tipo di controllo:

- Obiettivi
- Processo
- Casi d'uso
- Tecnologia
- Risultati aziendali

Obiettivi

- I controlli reattivi consentono di creare runbook per tipi di attacchi comuni, come il phishing o la forza bruta.
- I controlli reattivi consentono di implementare risposte automatizzate a potenziali problemi di sicurezza.
- I controlli reattivi possono porre automaticamente rimedio ad azioni non intenzionali o non approvate sulle AWS risorse, come l'eliminazione di bucket S3 non crittografati.

- I controlli reattivi possono essere orchestrati in modo da integrarsi ai controlli preventivi e di rilevamento al fine di creare un approccio olistico e proattivo per affrontare potenziali incidenti di sicurezza.

Processo

I controlli di rilevamento sono un prerequisito per stabilire controlli reattivi. È necessario essere in grado di individuare il problema di sicurezza prima di poterlo risolvere. e successivamente stabilire una policy o una risposta al problema. Ad esempio, in caso di attacco di forza bruta, si dovrebbe implementare un processo di correzione. Dopo aver completato l'operazione, il processo di correzione può essere automatizzato ed eseguito come script utilizzando un linguaggio di programmazione, ad esempio uno script della shell.

Valuta se il controllo reattivo potrebbe interrompere un carico di lavoro di produzione esistente. Ad esempio, se il controllo di sicurezza di rilevamento segnala che i bucket S3 non devono essere accessibili al pubblico e la correzione consiste nel disattivare l'accesso pubblico per Amazon S3, ciò potrebbe avere implicazioni significative per l'azienda e i clienti. Se il bucket S3 è presente in un sito Web pubblico, la disattivazione dell'accesso pubblico potrebbe causare un'interruzione. I database costituiscono un esempio simile. Se un database non deve essere accessibile pubblicamente tramite Internet, la disattivazione dell'accesso pubblico potrebbe influire sulla connettività all'applicazione.

Casi d'uso

- Risposta automatica agli eventi di sicurezza rilevati
- Correzione automatica delle vulnerabilità di sicurezza rilevate
- Controllo di ripristino automatico per ridurre i tempi di inattività operativa

Tecnologia

Security Hub

AWS Security Hubinvia automaticamente tutti i nuovi risultati e tutti gli aggiornamenti dei risultati esistenti agli eventi. EventBridge Puoi anche creare azioni personalizzate che inviano risultati selezionati e risultati di approfondimenti a EventBridge. Puoi configurare EventBridge per rispondere a ogni tipo di evento. L'evento può avviare una AWS Lambda funzione che esegue l'azione di riparazione.

AWS Config

AWS Configutilizza regole per valutare le AWS risorse e aiuta a correggere le risorse non conformi. AWS Config applica la riparazione utilizzando l'automazione.AWS Systems Manager Nei documenti di automazione, si definiscono le azioni che si desidera eseguire sulle risorse che si AWS Config ritiene non conformi. Dopo aver creato i documenti di automazione, è possibile utilizzarli in Systems Manager tramite AWS Management Console o utilizzando le API. Puoi scegliere di correggere manualmente o automaticamente le risorse non conformi.

Risultati aziendali

Minimizzazione della perdita di dati

Dopo un incidente di sicurezza informatica, l'utilizzo di controlli di sicurezza reattivi può aiutare a ridurre al minimo la perdita di dati e i danni al sistema o alla rete. I controlli reattivi possono anche consentire di ripristinare il più rapidamente possibile i sistemi e i processi aziendali critici, aumentando la resilienza dei carichi di lavoro.

Riduzione dei costi

L'automazione riduce i costi associati alle risorse umane perché i membri del team non devono rispondere manualmente agli incidenti o gestirli in altro modo. case-by-case

Passaggi successivi

La lettura di questa sezione dovrebbe consentirti di acquisire familiarità con i quattro tipi di controlli di sicurezza, comprendere il modo in cui fanno parte del framework di governance della sicurezza e iniziare a implementare e automatizzare i controlli di sicurezza nel Cloud AWS. Per ulteriori informazioni, ti consigliamo di rivedere i documenti di riferimento inclusi nella sezione Risorse.

Ti consigliamo inoltre di eseguire i passaggi seguenti per valutare la sicurezza dell'infrastruttura cloud e iniziare a implementare i controlli di sicurezza:

1. Abilita e configura AWS Security Hub. Come best practice, ti consigliamo di abilitare i controlli standard disponibili. Per ulteriori informazioni, consulta la pagina Controlli e standard di sicurezza (documentazione di Security Hub).
2. Abilita e configura AWS Config. Per ulteriori informazioni, consulta Nozioni di base (documentazione di AWS Config).
3. Utilizza i Servizi AWS, ad esempio Security Hub, Amazon Macie, AWS Config, AWS Trusted Advisor e Amazon Inspector per valutare l'organizzazione e l'infrastruttura dell'account, identificare le aree che richiedono miglioramenti ed esaminare i consigli su questi servizi. Utilizza la funzionalità di controllo di sicurezza in Security Hub per generare un punteggio di sicurezza per uno standard di sicurezza. Per ulteriori informazioni, consulta la pagina Definizione dei punteggio di sicurezza (documentazione di Security Hub).
4. Implementa i controlli di sicurezza preventivi, proattivi, di rilevamento e reattivi in base ai miglioramenti identificati.
5. Effettua una valutazione di follow-up per valutare l'efficacia dei controlli di sicurezza implementati. In Security Hub, determina se il punteggio di sicurezza è migliorato, quindi ripeti l'operazione per ottimizzare i controlli di sicurezza o aggiungerne di nuovi.
6. Stabilisci una cadenza regolare per l'esecuzione delle valutazioni di sicurezza, ad esempio una volta all'anno.

Domande frequenti

Su cosa devo concentrarmi se ho tempo e risorse limitate e non posso implementare tutti questi tipi di controllo?

Ti consigliamo di implementare AWS Security Hub. Security Hub dispone di una serie di controlli di sicurezza automatizzati denominati Standard di best practice per la sicurezza di base AWS (documentazione di Security Hub). Si tratta di un insieme altamente curato di best practice di sicurezza gestito agli esperti di sicurezza AWS. Puoi eseguire questi controlli standard in modo continuo, ogni volta che vengono apportate modifiche alle risorse associate, o periodicamente, secondo una pianificazione regolare. Ogni controllo ha un punteggio di gravità specifico per aiutarti a stabilire le priorità delle operazioni correttive. Per ulteriori informazioni, consulta la pagina Esecuzione dei controlli di sicurezza (documentazione di Security Hub). Se utilizzi AWS Control Tower, puoi anche esaminarlo e scegliere di abilitarne i controlli preventivi, di rilevamento e proattivi.

Risorse

Documentazione AWS

- Architettura di riferimento per la sicurezza di AWS (AWS SRA)
- Prospettiva di sicurezza CAF di AWS
- Best practice per la sicurezza, l'identità e la conformità
- Risposta di sicurezza automatizzata su AWS (soluzione AWS)
  - Pagina di destinazione della soluzione
  - Guida all'implementazione

Post del blog su AWS

- Guida a Identity - Controlli preventivi con AWS Identity - SCP
- Come implementare una policy di controllo dei servizi (SCP) di sola lettura per gli account in AWS Organizations
- Best practice per le policy di controllo dei servizi AWS Organizations in un ambiente multi-account
- Mantenere la conformità utilizzando le policy di controllo dei servizi e assicurarsi che vengano sempre applicate
- Quando e dove utilizzare i limiti delle autorizzazioni IAM
- Mantieni in modo proattivo le risorse sicure e conformi agli hook AWS CloudFormation

Altre risorse

- Cloud Controls Matrix (CCM) (Cloud Security Alliance)
- Limiti delle autorizzazioni di esempio (GitHub)

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
Controlli proattivi	Abbiamo aggiunto informazioni sui controlli proattivi a questa guida, inclusa la sezione Controlli proattivi.	4 dicembre 2023
Pubblicazione iniziale	—	12 dicembre 2022

AWS Glossario delle linee guida prescrittive

I seguenti sono termini comunemente usati 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 tuo database Oracle locale a Oracle su un'istanza EC2 in. 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. Esegui 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 frequentemente 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 viene utilizzato AIOps nella strategia di migrazione AWS , 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 for 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.

CoE

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 del 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 i post di CCoE 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 dimensionare l'adozione del cloud (ad esempio, creazione di una zona di destinazione, definizione di un CCoE, 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 del 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 o AWS CodeCommit. 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, AWS Panorama offre dispositivi che aggiungono CV alle reti di telecamere locali e Amazon SageMaker 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, creazione, test, gestione temporanea e produzione del processo di rilascio del software. Il processo CI/CD è comunemente descritto come una pipeline. CI/CD può aiutare ad automatizzare i processi, migliorare la produttività, migliorare

la qualità del codice e velocizzare le distribuzioni. 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, è possibile AWS CloudFormation utilizzarlo per rilevare deviazioni nelle risorse di sistema oppure AWS Control Tower per rilevare cambiamenti nella 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.

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.

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 la 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 in uno 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, vedere 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.

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.

G

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.

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 livello elevato che consente di governare risorse, policy e conformità tra le unità organizzative (OU). 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.

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, ad esempio 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. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e 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.

Internet delle cose industriale (IIoT)

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, consulta Creazione di una strategia di trasformazione digitale dell'Internet delle cose industriale (IIoT).

VPC di ispezione

In un'architettura AWS multi-account, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPC (uguali o diversi Regioni AWS), Internet e reti locali. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione 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, consulta la sezione Interpretabilità dei modelli 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.

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.

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 piccolo servizio indipendente che comunica tramite API ben definite ed è in genere di proprietà di piccoli team autonomi. 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 tramite un'interfaccia ben definita utilizzando API leggere. 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 includono in genere 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 AWS con 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.

O

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. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione 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 all'ingegneria dei sistemi che tiene conto della privacy durante l'intero processo di progettazione.

zone ospitate private

Un container che contiene informazioni su come si desidera che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più VPC. 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.

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.

pubblica/sottoscrivi (pub/sub)

Un pattern 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).

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 il 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. Ciò determina quella che viene considerata 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.

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.

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 Amazon EC2 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 policy che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in AWS Organizations. Le SCP definiscono i guardrail o fissano i limiti alle azioni che un amministratore può delegare a utenti o ruoli. Puoi utilizzare le SCP 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.

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 è possibile utilizzare per collegare i VPC e le reti on-premise. 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 VPC che consente di instradare il traffico tramite 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 interrogazioni 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.

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.