Crawl, walk, run: Accelerazione della maturità della sicurezza nel Cloud AWS

AWS Guida prescrittiva

AWS Guida prescrittiva: Crawl, walk, run: Accelerazione della maturità della sicurezza nel Cloud AWS

Table of Contents

Crawl, walk, run: accelerazione della maturità della sicurezza nel Cloud AWS

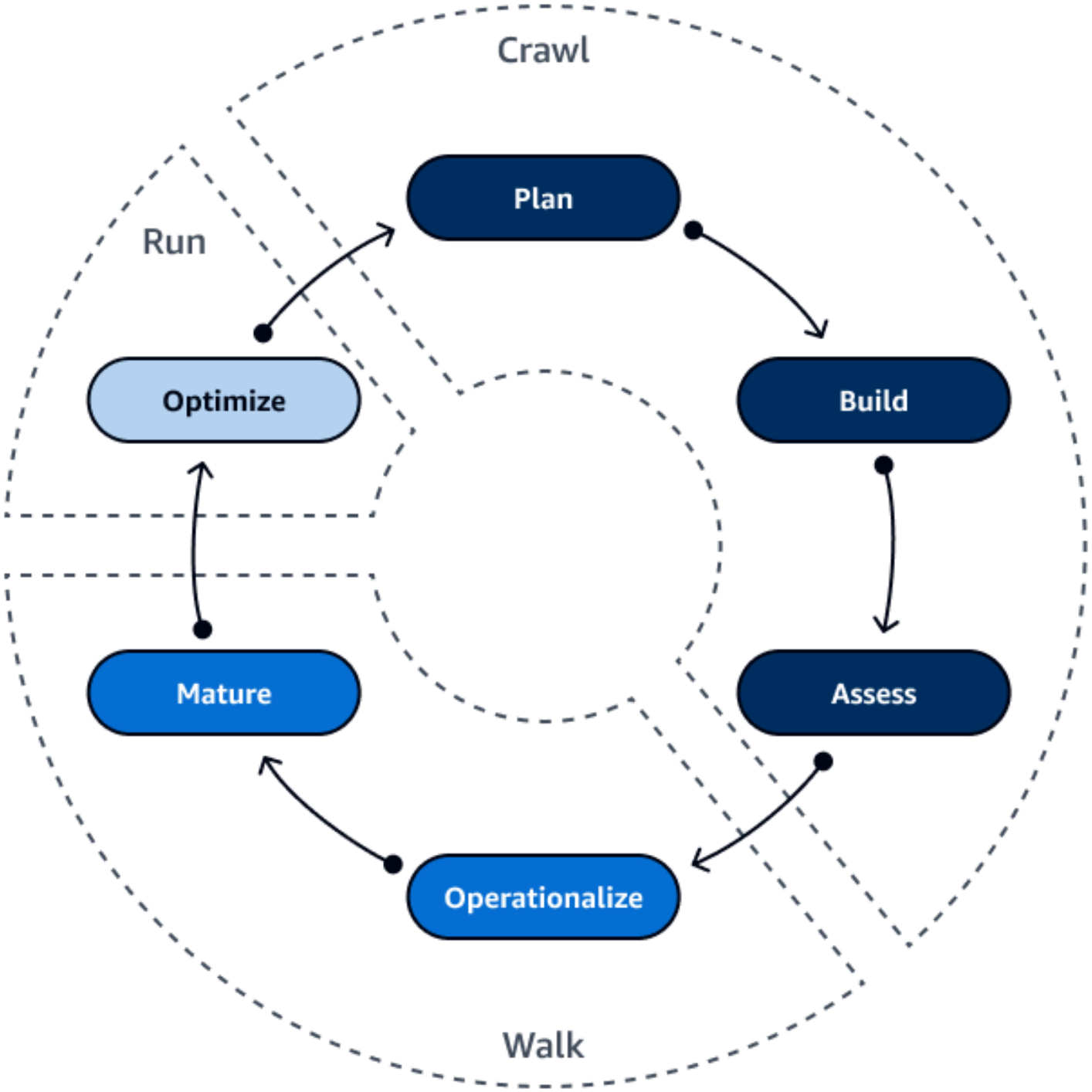
Amazon Web Services (collaboratori)

Dicembre 2023 (cronologia dei documenti)

Per molte organizzazioni, la sicurezza è la priorità e la considerazione numero uno durante la migrazione al cloud. L'implementazione delle funzionalità e dei controlli di sicurezza del cloud non è un'attività una tantum, ma un modello iterativo. Aumentate gradualmente il livello di sicurezza e la maturità man mano che aumentate le operazioni sul cloud. Ad esempio, potreste iniziare con politiche AWS gestite e poi, quando l'organizzazione sarà pronta, implementare politiche personalizzate che seguano il principio del privilegio minimo.

Questa guida fornisce una tabella di marcia per l'utilizzo di una metodologia crawl, walk, run per accelerare la maturità dell'organizzazione nella sicurezza del cloud. Definisce un step-by-step approccio per automatizzare le funzionalità di sicurezza. Spiega inoltre in modo pragmatico come sfruttare al massimo le funzionalità e le caratteristiche. Servizi AWS Questa guida ti aiuta a comprendere le sfide e le opportunità del cloud e come andare avanti rapidamente e raggiungere il successo con. AWS

Un percorso verso il cloud richiede la creazione di framework, la gestione e la maturazione delle operazioni e l'ottimizzazione dei processi. L'immagine seguente mostra le fasi di ogni fase della metodologia crawl, walk, run: pianificazione, costruzione, valutazione, operazionalizzazione, maturazione e ottimizzazione.



La fase di esplorazione consiste nella pianificazione, nella creazione delle fondamenta e nella valutazione dell'attuale livello di sicurezza. Nella fase iniziale, si rendono operativi il personale, i processi e la tecnologia, quindi si maturano le operazioni attraverso la messa a punto e la misurazione. La fase di esecuzione consiste nell'ottimizzazione attraverso la valutazione e l'automazione.

Fase di esplorazione: pianificazione, costruzione e valutazione

La fase di esplorazione inizia con la pianificazione. La pianificazione implica la determinazione dell'ambito di sicurezza e la scelta del modello più adatto all'organizzazione. Dopo aver stabilito il piano, puoi iniziare a costruire una base. Segue una valutazione del vostro attuale livello di sicurezza e l'impostazione di una disciplina non appena create l'infrastruttura di sicurezza. La fase di esplorazione è iterativa. L'iterazione nel cloud è più veloce dell'iterazione in un ambiente locale. Man mano che maturano le funzionalità del cloud, il processo di iterazione accelera.

Le seguenti sono le fasi della fase di esplorazione:

- Pianificazione— Come si determina l'ambito e si seleziona un modello?
- Creazione— Come intendi stabilire il quadro?
- Valutazione— Qual è la tua attuale posizione in materia di sicurezza?

Piano: definizione dell'ambito e del modello di sicurezza

La pianificazione è un processo iterativo man mano che il modello di sicurezza matura. Le fasi chiave del processo di pianificazione includono:

- Comprendere l'ambito della sicurezza— L'ambito di sicurezza varia e dipende da come viene utilizzato il cloud.
- Scelta di un modello di sicurezza— Identifica il modello di sicurezza più adatto al tuo caso d'uso in materia di sicurezza.
- Creazione di un modello di obiettivi aziendali— Definisci obiettivi e meccanismi chiari per misurare il successo.

Mentre sviluppi il tuo piano, considera quanto segue:

- Siate disposti a iterare. L'iterazione è costante nel cloud. L'iterazione ti aiuta a identificare le lacune nel piano.
- Non iniziate con i servizi. Inizia con il tuo piano invece di scegliere i servizi di cui hai bisogno. Questo aiuta a guidare l'organizzazione verso i risultati previsti.

Comprendere l'ambito della sicurezza

Il modello di responsabilità AWS condivisa definisce il modo in cui condividi la responsabilità AWS per la sicurezza e la conformità nel cloud. AWS protegge l'infrastruttura che gestisce tutti i servizi offerti nel e l' Cloud AWS utente è responsabile della protezione dell'uso di tali servizi, come dati e applicazioni.

Questo modello condiviso può contribuire ad alleggerire la conformità e l'onere operativo perché AWS gestisce, gestisce e controlla molti componenti, dal sistema operativo host e dal livello di virtualizzazione fino alla sicurezza fisica delle strutture in cui opera il servizio. I servizi gestiti aiutano a ridurre gli obblighi di sicurezza e conformità consentendo di AWS gestire alcune attività di sicurezza, come l'applicazione di patch e la gestione delle vulnerabilità. L'utilizzo di servizi gestiti è una best practice nel AWS Well-Architected Framework. In generale, man mano che l'infrastruttura viene modernizzata, maggiori responsabilità vengono trasferite sul fornitore di servizi.

Di seguito sono riportati tre diversi esempi di servizi per aiutarvi a capire come cambia l'ambito di sicurezza in base ai servizi scelti:

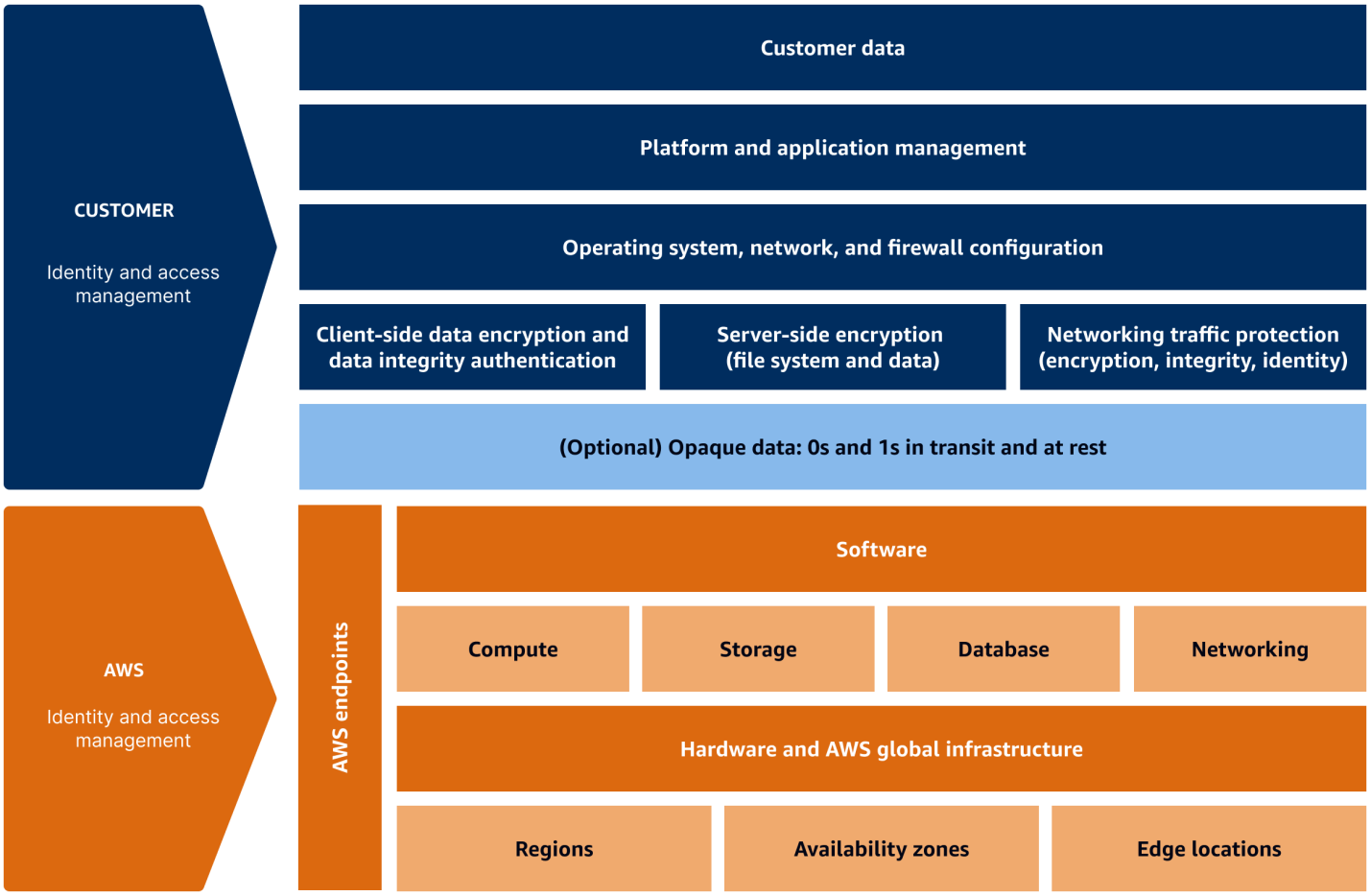
- Servizi di infrastruttura
- Servizi di container
- Servizi serverless

La responsabilità dell'utente in materia di sicurezza non è statica e cambia in base al tipo di architettura selezionato. Il tuo tempo, il tuo impegno e i tuoi costi sono influenzati dall'architettura cloud che scegli.

Servizi di infrastruttura

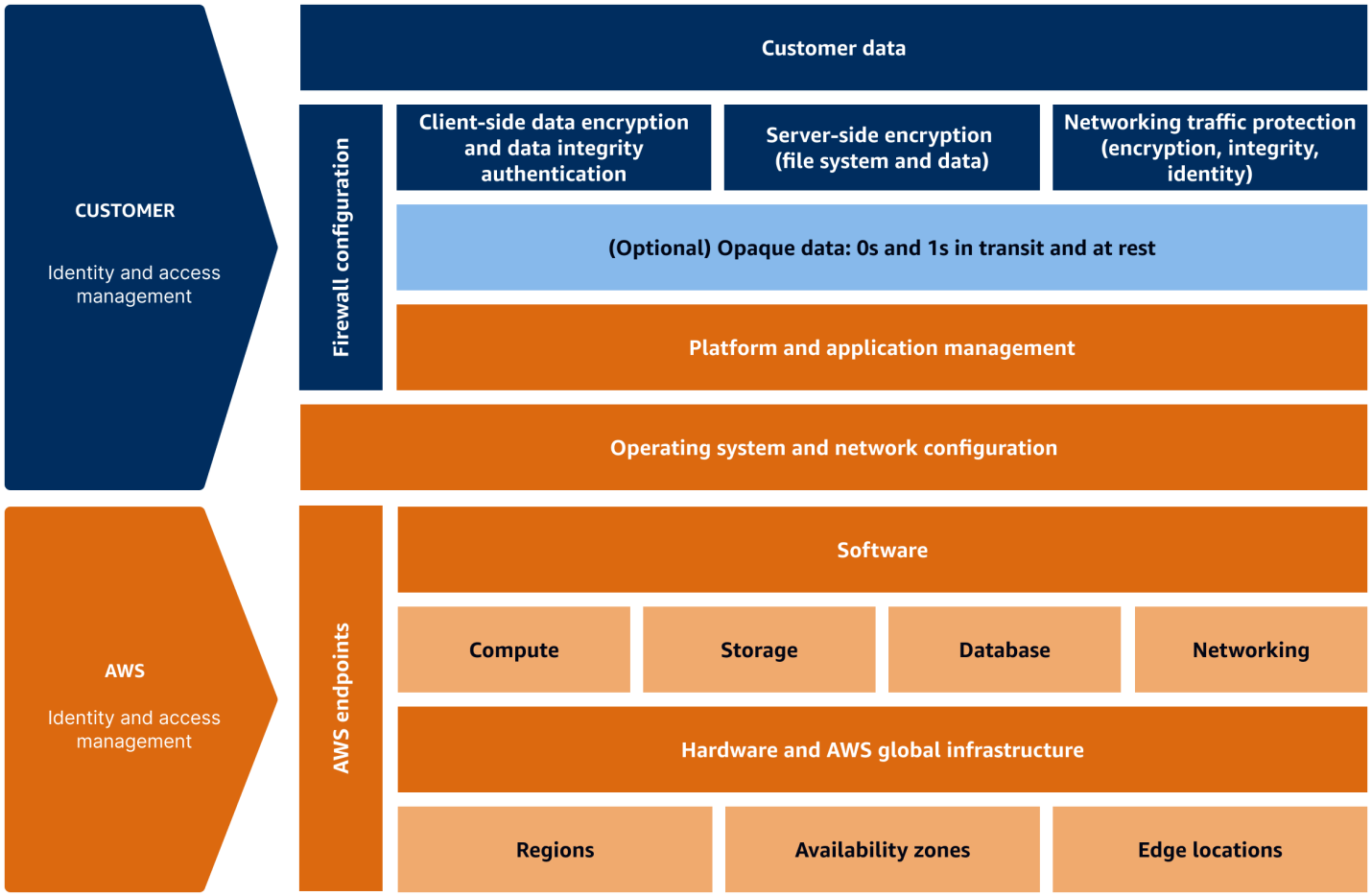
Per quanto riguarda i servizi di infrastruttura, AWS si concentra sulla protezione dell'infrastruttura sottostante. Nell'ambito dei servizi di infrastruttura, l'ambito è più ampio per il cliente, in quanto, rispetto agli altri modelli, deve occuparsi della sicurezza della piattaforma, dell'applicazione di patch al

sistema operativo e della gestione delle applicazioni. Amazon Elastic Compute Cloud (Amazon EC2) Elastic Compute Cloud (Amazon EC2) è un esempio di servizio di infrastruttura comune.



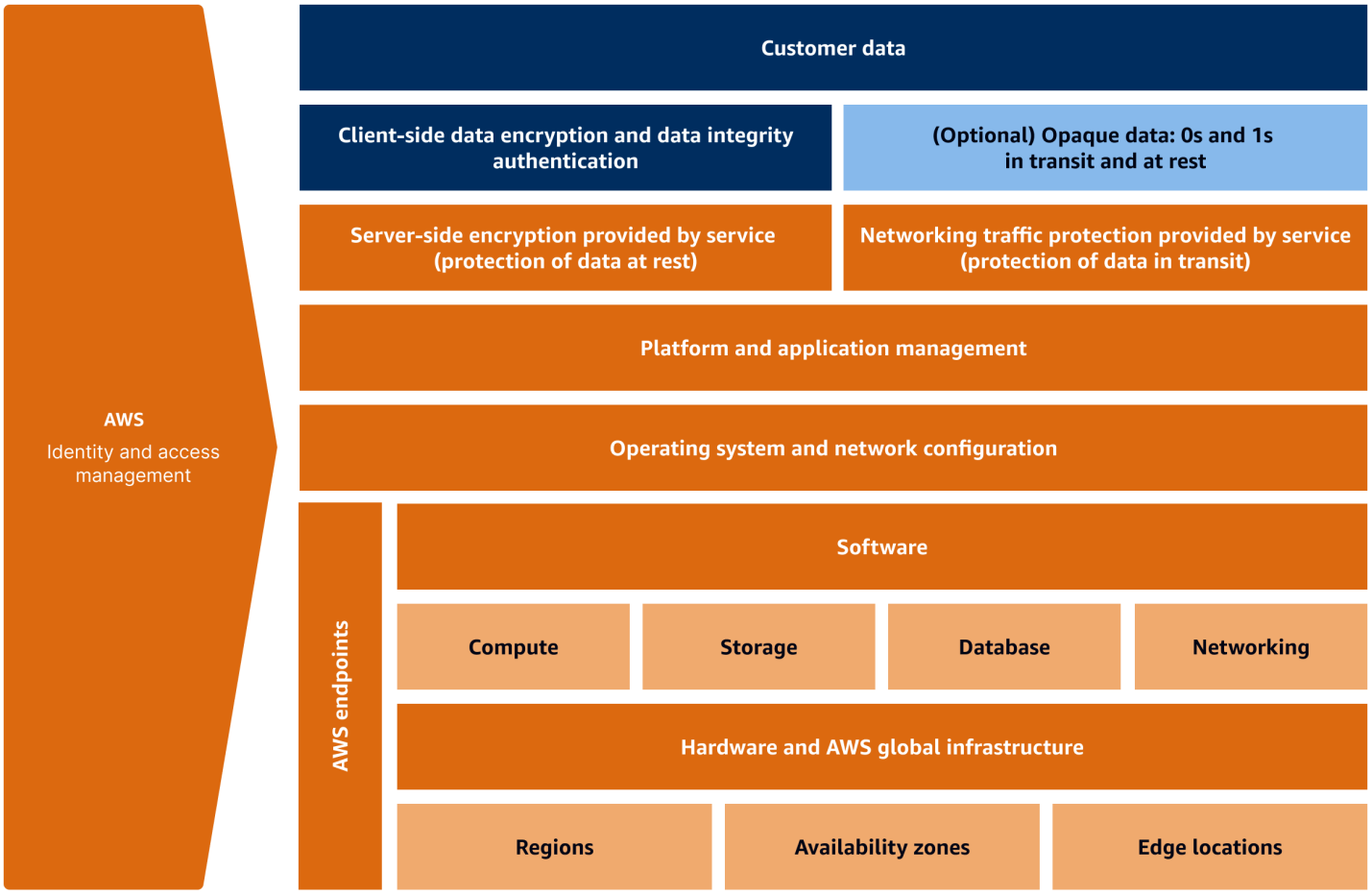
Servizi di container

Man mano che l'infrastruttura diventa più astratta e modernizzata, l'ingombro si riduce. Il tuo ambito si restringe perché la responsabilità di alcuni elementi di sicurezza si sposta verso. AWS I servizi di container sono un esempio a cui tornano alcune responsabilità di backend. AWS Ad esempio, AWS diventa responsabile della configurazione del sistema operativo (OS), della configurazione di rete, della gestione della piattaforma e della gestione delle applicazioni. Esempi di servizi container comuni includono Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Registry (Amazon ECR), Amazon Elastic Container Service (Amazon ECS) e. AWS Fargate



Servizi serverless

Quando si utilizzano servizi serverless, quasi tutta la responsabilità della sicurezza appartiene a. AWS L'ambito della tua responsabilità è minimo. Ad esempio, un database serverless gestito (DB) elimina la necessità di proteggere la rete, l'hardware e il sistema operativo. Tutte le patch del sistema operativo e del DB sono coperte da. AWS La tua unica preoccupazione è proteggere l'accesso ai dati tramite crittografia e autenticazione.



Scelta di un modello di sicurezza

Puoi scegliere tra vari modelli o approcci di sicurezza per AWS. La scelta dell'approccio e del modello più adatto dipendono dal pubblico, dai risultati aziendali target e dal processo aziendale complessivo. È possibile utilizzare una combinazione di più modelli.

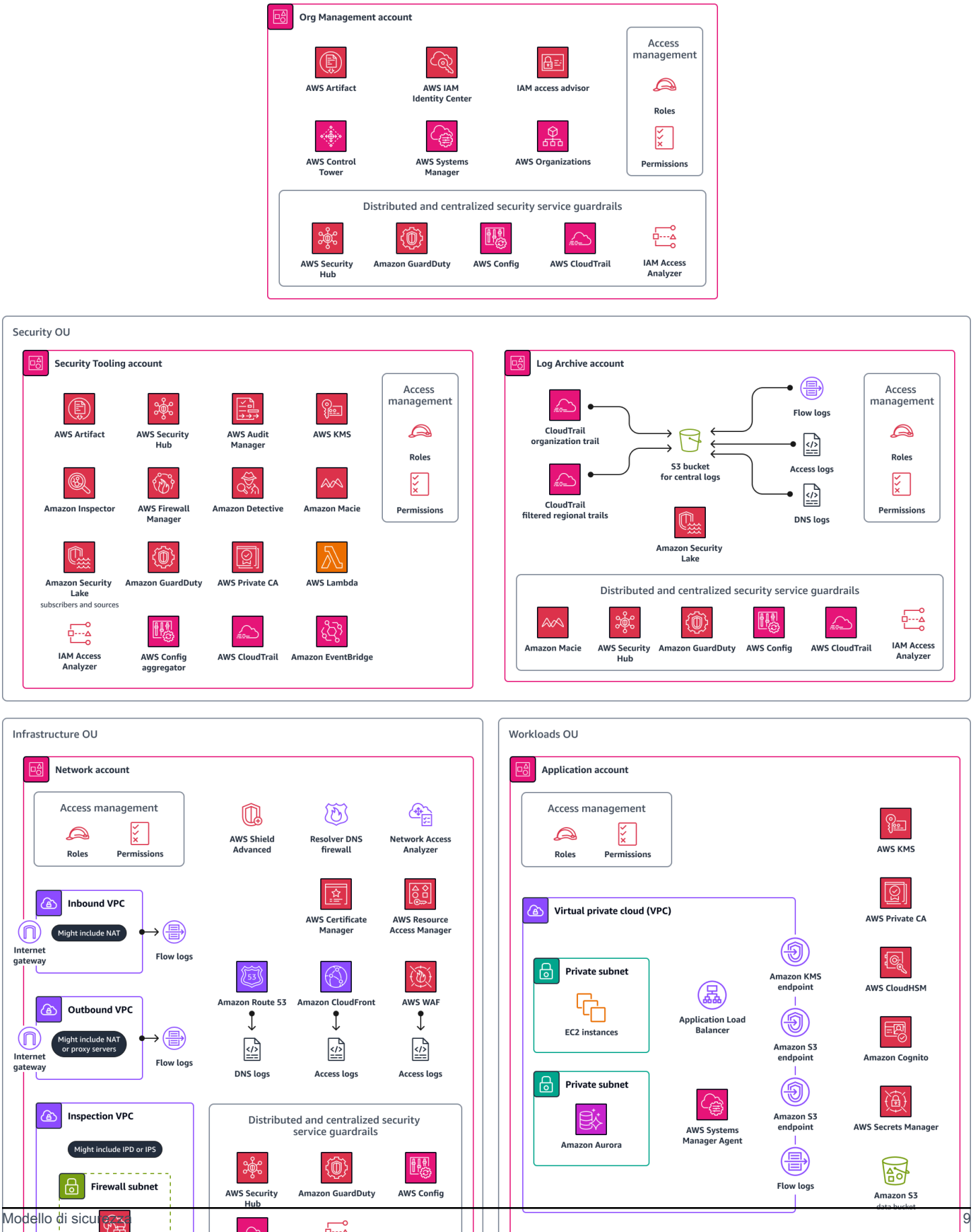
Di seguito sono riportati alcuni modelli comuni:

- Modello architettonico
- Modello di maturità
- Modello di governance

Ogni modello presenta una serie di vantaggi e svantaggi. È importante considerare quale approccio è più adatto alla propria organizzazione. Coinvolgi i professionisti della sicurezza nelle prime fasi del processo di modernizzazione dell'infrastruttura e adozione delle strategie cloud. Il modello scelto ha un impatto significativo sui ruoli e le responsabilità all'interno dell'organizzazione.

Modello architettonico

L'immagine seguente mostra la AWS Security Reference Architecture. Questo approccio architettonico fornisce un modello per un modello di sicurezza. Questo approccio è più adatto quando si interagisce con i team tecnici dell'organizzazione. Aiuta a stabilire un obiettivo ideale per lo stato futuro. Inoltre, è in linea con molti framework e conformità. AWS


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Access management
Roles
Permissions
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
Amazon Security Lake
subscribers and sources
Amazon GuardDuty
AWS Private CA
AWS Lambda
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
Amazon Security Lake
Access management
Roles
Permissions
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Certificate Manager
AWS Resource Access Manager
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Workloads OU
Application account
Access management
Roles
Permissions
AWS KMS
Virtual private cloud (VPC)
AWS Private CA
Private subnet
EC2 instances
Application Load Balancer
Amazon KMS endpoint
AWS CloudHSM
Amazon S3 endpoint
Amazon Cognito
Private subnet
Amazon Aurora
AWS Systems Manager Agent
Amazon S3 endpoint
AWS Secrets Manager
Flow logs
Amazon S3
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Vantaggi del modello architettonico:

- Si allinea ai requisiti dell'Health Insurance Portability and Accountability Act (HIPAA) e dell'Health Information Trust Alliance Common Security Framework (HITRUST CSF)
- Fornisce una prospettiva architettonica
- Si allinea alle strategie e alle linee guida cloud per le grandi imprese
- Si allinea al AWS Cloud Adoption Framework (CAF)AWS
- Si allinea con il AWS Well-Architected Framework

Svantaggio del modello architettonico:

- È incentrato sulla tecnologia anziché sul business

Modello di maturità

L'approccio del AWS Security Maturity Model si concentra sulla gestione e la riduzione dei rischi dando priorità all'implementazione delle misure di sicurezza. Questo approccio è adatto ai responsabili della sicurezza CISOs, ma non è incentrato sul business.

Vantaggi del modello di maturità:

- È incentrato sulla sicurezza
- È un modello che si concentra sull'utilizzo di un approccio di implementazione basato sull'agilità
- Ti aiuta a ridurre rapidamente i rischi
- Si allinea al AWS Cloud Adoption Framework (AWS CAF)

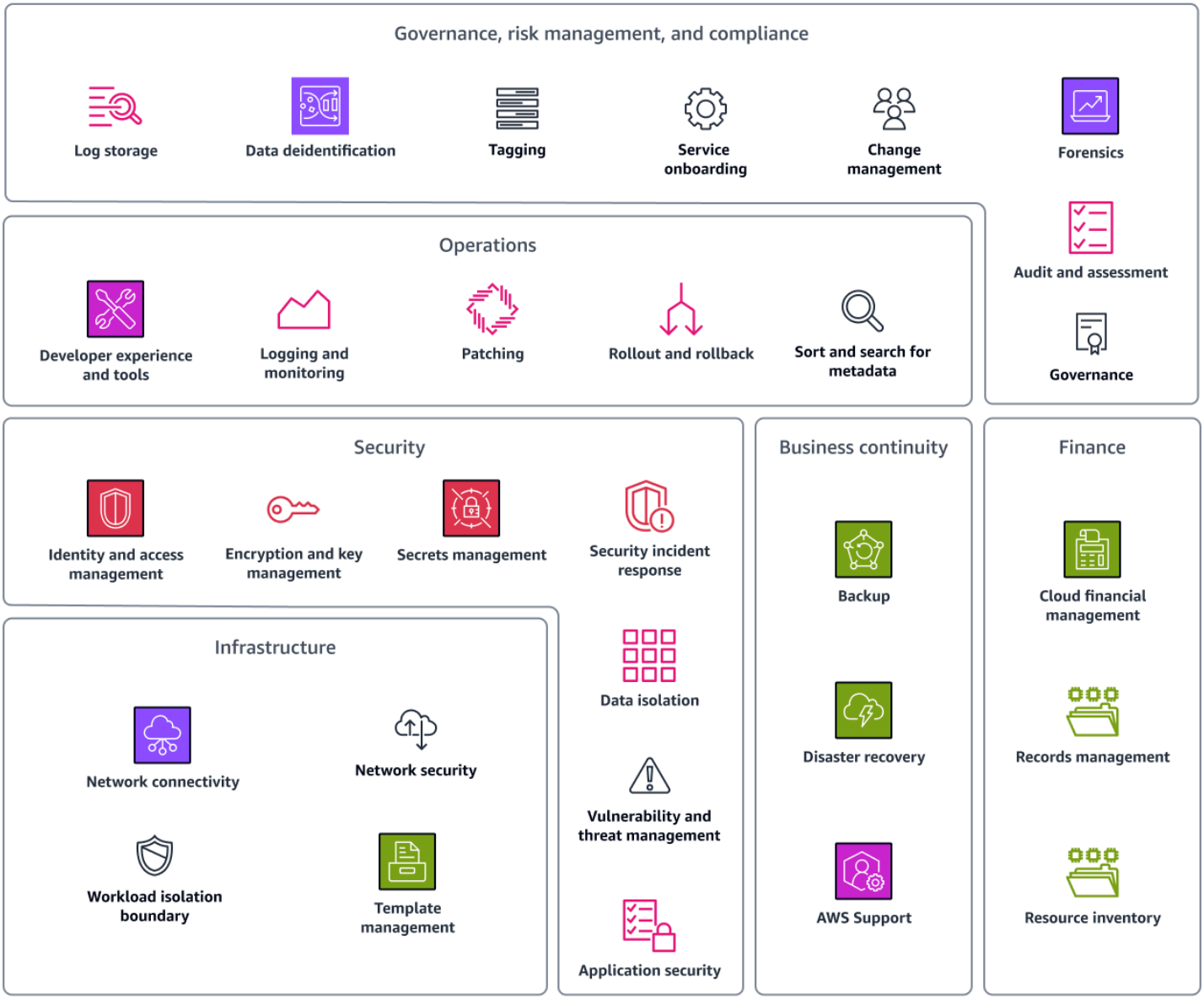
Svantaggi del modello di maturità:

- È incentrato sulla tecnologia anziché sul business

Modello di governance

Il AWS modello Cloud Foundation utilizza un approccio di governance, gestione del rischio e conformità (GRC) per aiutare le organizzazioni a soddisfare i requisiti di sicurezza e conformità. Definisce le politiche generali che l'ambiente cloud deve seguire. Le funzionalità di questo modello

consentono di definire le azioni da intraprendere, definire la propensione al rischio e allineare le politiche interne.



Il modello Cloud Foundation è una guida alle funzionalità e alla governance che ti aiuta a creare ed evolvere il tuo Cloud AWS ambiente. Si basa su una serie di definizioni, scenari, linee guida e automazioni. La guida include gli aspetti relativi alle persone, ai processi e alla tecnologia relativi alla creazione di un Cloud AWS ambiente. Copre sei categorie di funzionalità essenziali per una base cloud:

- Governance, gestione del rischio e conformità
- Operazioni

- Sicurezza
- Continuità aziendale
- Ambito finanziario
- Infrastruttura

La guida fornisce anche esempi, tempistiche e ulteriori letture per ciascuna funzionalità.

Vantaggi del modello di governance:

- Ha un ampio focus tecnologico
- È progettato per l'affidabilità
- Utilizza un approccio operativo

Svantaggio del modello di governance:

- È incentrato sulla tecnologia anziché sul business

Creazione di un modello di obiettivi aziendali

Il modello degli obiettivi aziendali prevede la definizione dei risultati aziendali. È simile al AWS Cloud Adoption Framework e al AWS Well-Architected Framework. Questo approccio si concentra su ciò a cui l'azienda è interessata interpretando i risultati aziendali target. Il valore di questo approccio è che è facile collegare gli obiettivi aziendali agli obiettivi di sicurezza. Un esempio di obiettivo aziendale è «Abilitare connessioni esterne sicure e accelerare il provisioning di nuovi utenti e ambienti, automatizzando la visibilità e misurando le migliori pratiche per ridurre continuamente i rischi». Stabilisci obiettivi tecnologici che ti aiutano a raggiungere i corrispondenti risultati aziendali. Il modello degli obiettivi aziendali si ricollega agli obiettivi di sicurezza, come il mantenimento della visibilità. Si implementa quindi un obiettivo tecnico, come le migliori pratiche di sicurezza AWS Identity and Access Management (IAM), al fine di ridurre i rischi per la sicurezza.

Vantaggi dell'approccio basato sugli obiettivi aziendali:

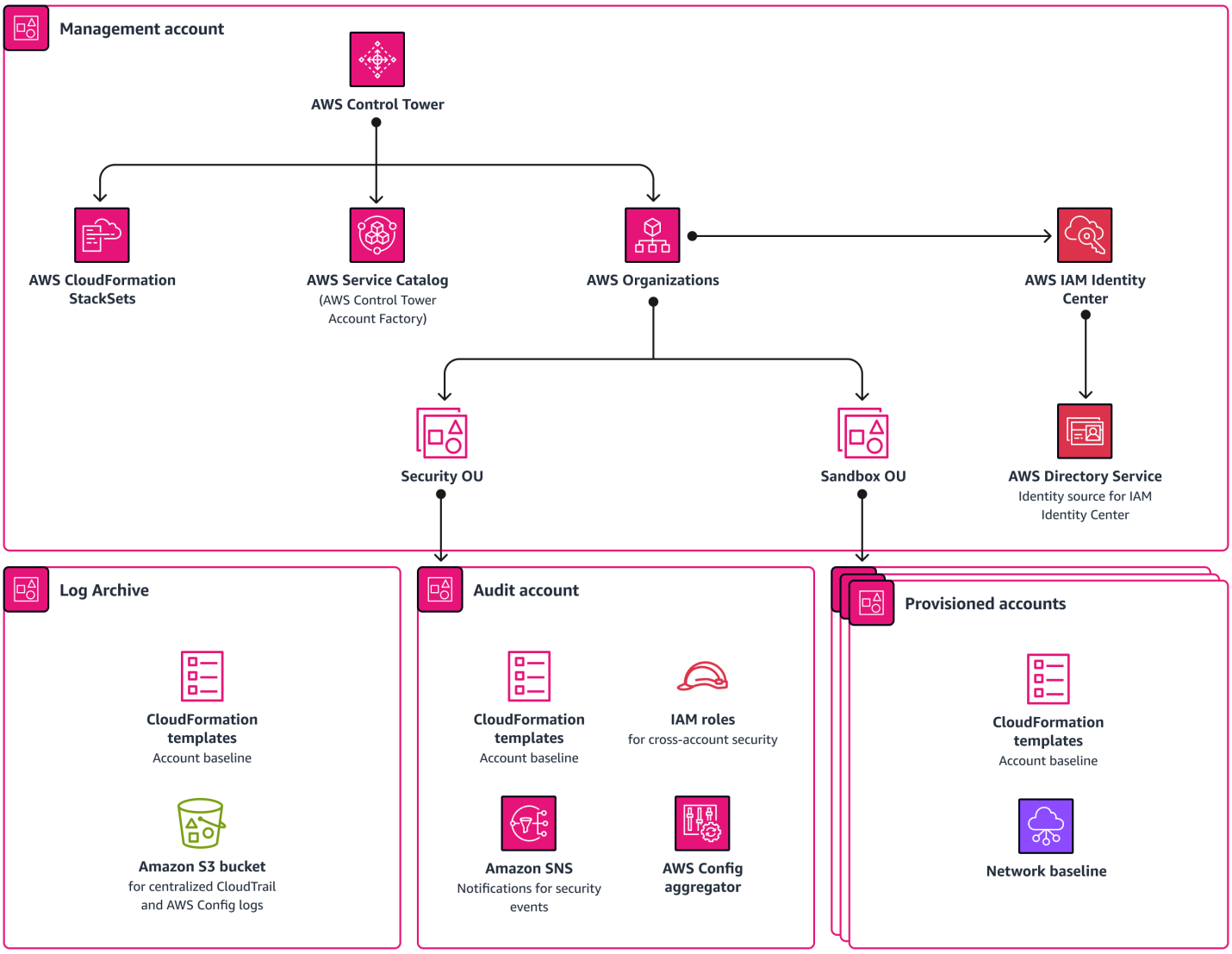
- Include la giustificazione dei costi
- Fornisce una direzione di sicurezza chiara e allineata al business
- Definisce le misure del successo attraverso il raggiungimento dei risultati aziendali prefissati

Svantaggi dell'approccio oggettivo aziendale:

- Può richiedere molto tempo perché devi capire cosa vuole l'azienda
- È incentrato sul business piuttosto che sulla tecnologia

Build: gettare le basi per una solida base di sicurezza del cloud

Ora che hai un piano, il passo successivo è gettare le basi. Questo passaggio dimostra come creare una base AWS cloud iniziale sicura, resiliente, scalabile e automatizzata su più account. La posa delle basi può essere progettata e personalizzata specificamente in base agli obiettivi aziendali. Puoi adattare i controlli a una nuova landing zone oppure puoi includerli in una landing zone esistente. Le automazioni integrate AWS Control Towerpossono aiutarti a gettare le basi di sicurezza in. Cloud AWS L'immagine seguente mostra una landing zone configurata attraverso AWS Control Tower.



AWS Control Tower orchestra più elementi per tuo Servizi AWS conto, ad esempio AWS Organizations AWS Service Catalog, e. AWS IAM Identity Center Puoi configurare una nuova landing zone entro un'ora e quella zona di atterraggio è progettata per soddisfare i tuoi requisiti di sicurezza e conformità. AWS Control Tower configura la landing zone in base alle migliori pratiche di sicurezza prescrittive. AWS Control Tower ti aiuta a gestire il cloud provisioning migliorando la visibilità e il controllo su account e utenti finali. Aiuta gli amministratori ad allocare e supervisionare in modo efficiente le risorse di elaborazione, implementare il controllo degli accessi basato sui ruoli, monitorare le prestazioni tramite strumenti di registrazione e monitoraggio, gestire efficacemente i costi, automatizzare i processi di implementazione, applicare misure di sicurezza e garantire la conformità agli standard di settore.

AWS Control Tower è il modo più veloce per configurare e gestire un ambiente sicuro, conforme e multi-account basato sulle migliori pratiche. AWS Per ulteriori informazioni su come lavorare AWS Control Tower e sulle migliori pratiche delineate nella strategia multi-account, consulta AWS Strategia AWS multi-account: linee guida sulle migliori pratiche.

Sebbene AWS Control Tower sia l'approccio più veloce, non è l'unico. L'importante è impostare una landing zone che, come minimo, fornisca quanto segue:

- Gestione di più account
- Gestione delle identità e degli accessi federati
- Un archivio centralizzato per i log
- Accesso di controllo su più account
- Fornitura di account per utenti finali
- Monitoraggio e notifiche centralizzati

Valutazione: valutazione della vostra attuale posizione in materia di sicurezza nel cloud

Prima di schierare qualcosa nella landing zone, valuta la zona di atterraggio per assicurarti che soddisfi i tuoi requisiti e stabilisci una linea di base. Questa pratica si chiama valutazione della postura nel cloud. Ti aiuta a identificare e correggere i rischi nell'infrastruttura cloud. La valutazione del livello di sicurezza del cloud offre la visibilità dei controlli di sicurezza pertinenti nell'ambiente cloud.

Di seguito sono riportati i vantaggi di una valutazione della postura nel cloud:

- Ti aiuta a comprendere il tuo attuale livello di sicurezza e a ottenere consigli per ridurre il tuo profilo di rischio, correggere le vulnerabilità esistenti o correggere configurazioni errate.
- Ti aiuta a identificare le migliori pratiche di sicurezza in modo da evitare errori e ridurre i rischi aziendali.
- Fornisce metriche che consentono di monitorare i miglioramenti e misurare il successo.

Questa sezione esamina i servizi AWS Security Hub CSPM e Prowler gli strumenti che puoi utilizzare per eseguire una valutazione della postura del cloud nel tuo ambiente.

Prowler

Prowlerè uno strumento a riga di comando open source che consente di valutare, controllare e monitorare gli account per verificarne la conformità alle migliori pratiche di AWS sicurezza e ad altri framework e standard di sicurezza. Ispeziona la configurazione e identifica i problemi di sicurezza. È possibile utilizzarlo Prowler in ambienti con più account e anche fornitori di terze parti possono utilizzarlo per valutare la sicurezza dell'ambiente. AWS

Di seguito sono riportati i vantaggi di: Prowler

- È gratuito e open source.
- Dispone di opzioni di implementazione flessibili ed è scalabile.
- Esegue controlli di conformità, ad esempio per Center for Internet Security (CIS) Benchmark for AWS, General Data Protection Regulation (GDPR) e HIPAA.
- Ti aiuta a creare istantanee e linee di base.

AWS Security Hub CSPM

AWS Security Hub CSPMfornisce una visione completa dello stato di sicurezza in. AWS Inoltre, consente di verificare la conformità dell'ambiente agli standard e alle best practice del settore della sicurezza. È integrato AWS Control Tower in modo da poter configurare i controlli investigativi CSPM di Security Hub tramite il AWS Control Tower servizio. L'obiettivo di accelerare la maturità della sicurezza è quello di far maturare il processo di valutazione da un'istantanea una tantum a un processo continuo per il monitoraggio dei progressi.

Di seguito sono riportati i vantaggi di Security Hub CSPM:

- Fornisce una dashboard unificata che mostra lo stato attuale dell'ambiente e aiuta a identificare e risolvere i problemi.
- Esegue valutazioni continue con controlli automatici.

Fase di marcia: operatività e maturazione

La fase di camminata si concentra sull'operatività. Durante questa fase, l'organizzazione deve valutare il suo attuale modello operativo, determinare come adattarlo al cloud, implementare tali modifiche e quindi misurare i progressi. Ciò include la valutazione delle competenze, dei processi operativi e della tecnologia. Ottimizzare l'implementazione del cloud e misurare i progressi è fondamentale durante tutta la fase iniziale per convalidare il successo.

Le seguenti sono le fasi della fase di camminata:

- Rendi operativa— Come preparate il personale, la tecnologia e i processi per il cloud?
- Maturo— Come si misurano i progressi e il successo?

Rendi operativa: prepara la tua organizzazione a un approccio maturo alla sicurezza del cloud

Per andare avanti con il processo di distribuzione dei carichi operativi nel cloud, è importante concentrarsi sull'allineamento di persone, processi e tecnologia. Ciò è particolarmente importante nell'ambiente cloud perché i processi e le competenze probabilmente differiscono dalle operazioni locali. In questa sezione, utilizzi un framework per allineare persone, processi e tecnologie, quindi confermi che il framework ti ha aiutato a raggiungere i risultati attesi.

AWS Framework di adozione del cloud

Il AWS Cloud Adoption Framework (AWS CAF) ti aiuta ad accelerare i risultati di business attraverso un uso Servizi AWS e funzionalità innovativi. AWS CAF identifica sei prospettive organizzative specifiche che sono alla base delle trasformazioni cloud di successo: Business, People, Governance, Platform, Security e Operations. Ogni prospettiva contiene funzionalità che possono migliorare la tua preparazione al cloud e aiutarti ad accelerare il tuo percorso di trasformazione nel cloud.

L'immagine seguente mostra le sei prospettive del AWS CAF e le funzionalità in ciascuna prospettiva. Per ulteriori informazioni, consulta le funzionalità di base in Una panoramica del Cloud Adoption Framework. AWS

Risultati attesi

Quando utilizzi il AWS CAF per allineare persone, processi e tecnologie, puoi aspettarti di ottenere i seguenti risultati:

- DevSecOps pipeline e processo: l'implementazione di una DevOps pipeline con strumenti di sicurezza integrati può aiutarvi a implementare in modo più sicuro l'infrastruttura come codice (IaC). È possibile implementare la scansione del codice e i controlli di sicurezza nel processo di pipeline, come cfn_nag (), che è un analizzatore di codice statico open source. GitHub
- Etichettatura e gestione delle risorse: i tag possono aiutarti a gestire in modo più efficiente e coerente le risorse nel cloud. Per ulteriori informazioni, consulta Tagging delle risorse AWS. È importante sviluppare una strategia di gestione delle risorse dinamica in grado di adattarsi alla natura in continua evoluzione del cloud. AWS Systems Manager Inventory ti aiuta ad assegnare tag in modo da poter cercare, gestire e identificare rapidamente le tue risorse.
- Monitoraggio e integrazione investigativa: è fondamentale stabilire un metodo per inviare avvisi dal cloud ai centri operativi di sicurezza locali (SOCs) e ai sistemi di gestione delle informazioni e degli eventi di sicurezza (SIEM). Amazon GuardDuty è un servizio di monitoraggio continuo della sicurezza che analizza ed elabora i log per identificare attività impreviste e potenzialmente non autorizzate nel tuo ambiente. AWS Si integra inoltre con molti strumenti di terze parti.
- Piano e programma di risposta agli incidenti nel cloud: è importante assicurarsi che il personale responsabile della gestione degli avvisi cloud abbia familiarità con il processo di acquisizione di tali avvisi e sappia come rispondere agli avvisi cloud, rispetto agli avvisi locali. Per migliorare le capacità di risposta agli incidenti, forma il personale a utilizzare Amazon Detective per l'analisi dei log. Amazon Detective ti aiuta ad analizzare, indagare e identificare la causa principale dei risultati di sicurezza o delle attività sospette. Amazon Detective dovrebbe far parte di un piano di risposta agli incidenti.
- Gestione delle vulnerabilità nel cloud: il processo di gestione delle vulnerabilità nel cloud è diverso da quello degli ambienti locali. Oltre alla tradizionale gestione delle vulnerabilità, è necessario valutare anche il livello di codice dell'infrastruttura. Amazon Inspector è un servizio automatizzato di gestione delle vulnerabilità che valuta continuamente le tue risorse per individuare eventuali vulnerabilità ed esposizione involontaria della rete.
- Gestione della postura nel cloud: la gestione della postura nel cloud, come descritto nella sezione Valutazione, è un aspetto importante della sicurezza del cloud. Puoi utilizzarlo AWS Security Hub CSPM per automatizzare i controlli delle migliori pratiche di sicurezza e valutare la tua posizione complessiva sul cloud in tutti i tuoi. Account AWS
- Formazione sulla sicurezza nel cloud: è essenziale fornire una formazione adeguata ai dipendenti in modo che acquisiscano competenze nella sicurezza del cloud. Ciò include l'accesso alle risorse e l'assegnazione del tempo ai dipendenti per acquisire le conoscenze e le competenze necessarie. AWS fornisce molte risorse di formazione per migliorare le competenze e l'istruzione, come AWS Skill Builder.

Maturo: ottimizzazione e misurazione di processi, strumenti e rischi

Nella fase matura del modello di sicurezza cloud, l'attenzione si concentra sull'allineamento dei team di sicurezza alle funzionalità di sicurezza del AWS Cloud Adoption Framework (AWS CAF) e sull'istituzione di processi agili. Questo allineamento aiuta i team specializzati ad accelerare l'innovazione in brevi sprint, incorporando al contempo tabelle di marcia e pianificazione a lungo termine. La fase matura enfatizza la collaborazione con le operazioni IT e lo sviluppo di competenze cloud approfondite e specializzate. Ogni funzionalità di sicurezza implementa strumenti e processi chiave per migliorare l'efficienza e l'impatto, accompagnata dallo sviluppo di metriche e meccanismi di reporting per misurare le modifiche incrementali e l'impatto complessivo.

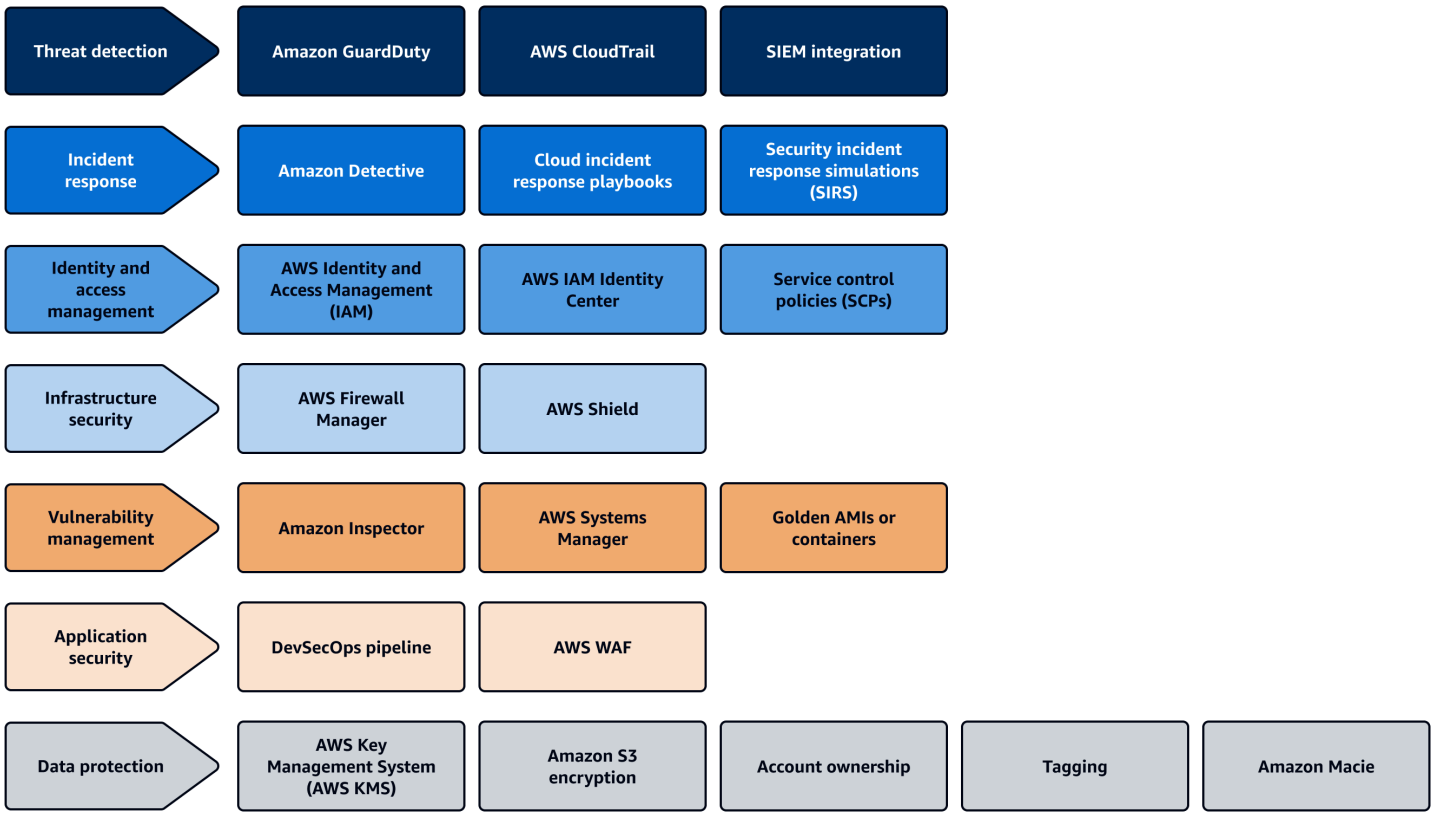
In questa fase, devi:

- Ottimizza e misura i processi
- Ottimizza e misura gli strumenti
- Ottimizza e misura il rischio
- Esamina esempi di casi d'uso nella fase matura

Ottimizza e misura i processi

L'approccio agile offre maggiore flessibilità e innovazione e può aiutarti a testare e implementare rapidamente nuove idee. Suddividi i team di sicurezza in ruoli specializzati, come quelli addetti alla risposta agli incidenti e i gestori delle vulnerabilità. I ruoli devono essere allineati alle categorie nell'immagine seguente, che corrispondono alle funzionalità del AWS Cloud Adoption Framework (AWS CAF). L'approccio agile incoraggia i team a pensare in grande, inventare, semplificare e identificare potenziali lacune nella sicurezza. Ciò si traduce nella creazione di un backlog di storie utente o tabelle di marcia per miglioramenti futuri.

Un processo agile consente soluzioni più dinamiche e adattive, anziché affidarsi esclusivamente alle capacità di uno strumento specifico. Fail fast è una filosofia che utilizza test frequenti e incrementali per ridurre il ciclo di vita dello sviluppo ed è una parte fondamentale di un approccio agile. Apporta una modifica, testala e poi decidi se continuare con l'approccio attuale o passare a uno alternativo. Se i team lavorano in questo ciclo, ciò aiuta l'organizzazione a rimanere al passo con la natura frenetica del cloud. Anche la formazione mirata è fondamentale e dovresti fornire una formazione specifica per un particolare dominio della sicurezza del cloud.



> **Note**
>
> Questa immagine non contiene le funzionalità di garanzia e governance della sicurezza del CAF. AWS Questa guida si concentra sulle operazioni di sicurezza e la garanzia e la governance della sicurezza non rientrano nell'ambito di questa guida. Per ulteriori informazioni sulla garanzia della sicurezza, consulta AWS re:INforce 2023 - Scaling compliance with on. AWS Control Tower YouTube

Nella tua organizzazione, utilizza un approccio agile che la aiuti a stare al passo con lo sviluppo e i cambiamenti rapidi nel cloud. Di seguito sono riportati alcuni modi per iniziare a sperimentare e iterare nel tuo ambiente cloud:

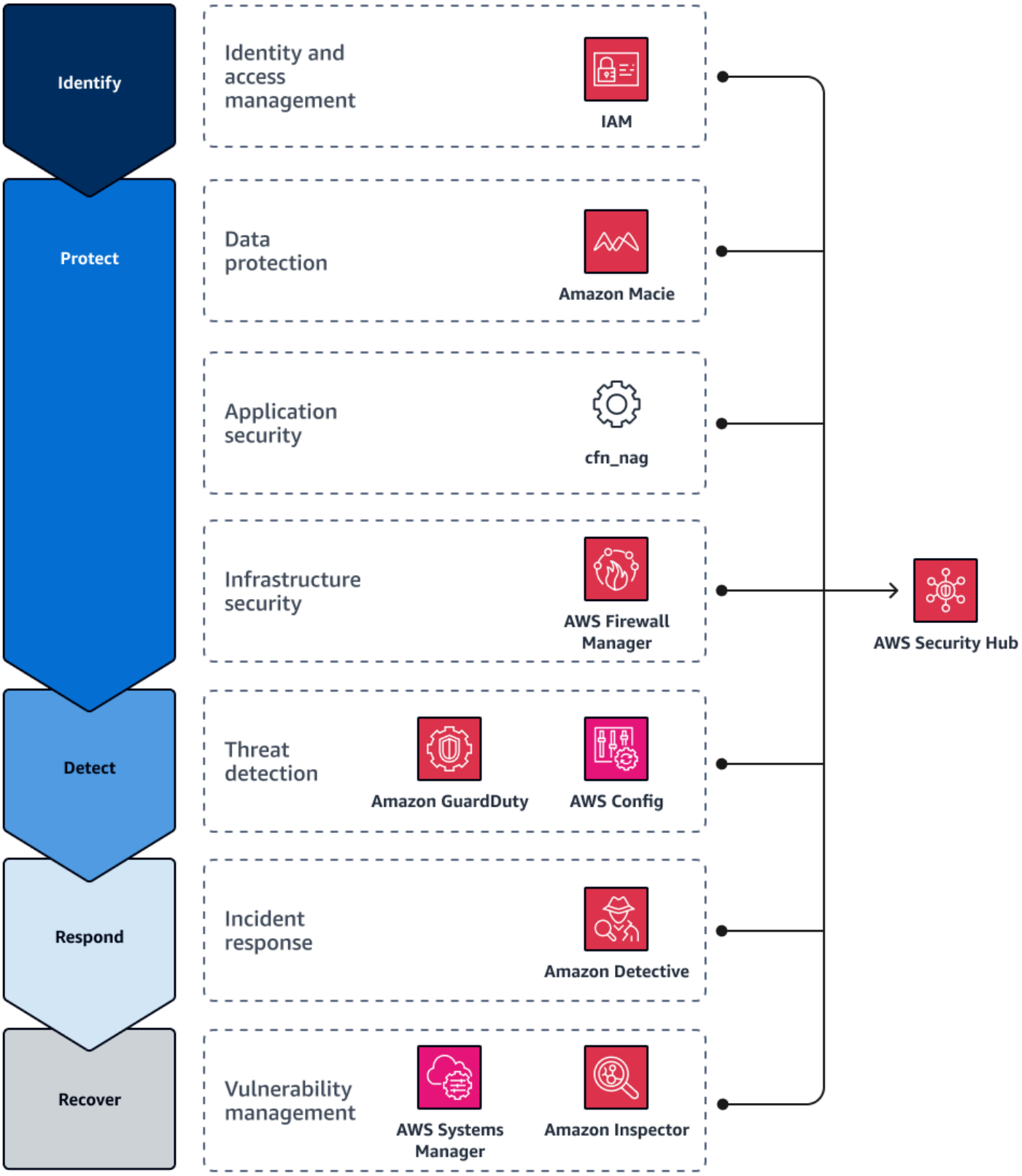
- Specializzati nelle categorie definite in AWS CAF, come mostrato nell'immagine precedente.
- Per essere più dinamici, concentratevi sull'innovazione anziché sulle operazioni.
- Agisci rapidamente negli sprint permettendo alle persone di testare, fallire rapidamente e implementare rapidamente e continuare con questo ciclo per stare al passo con il business.

- Per supportare operazioni continue, ove possibile, allinea i processi per ambienti basati su cloud e locali.
- Per aiutare le persone ad approfondire e concentrarsi su un'area, offri una formazione mirata anziché una formazione generale.
- Incoraggia le persone a pensare in grande, a indagare su «cosa succederebbe se» e a creare arretrati (ad esempio tabelle di marcia o lacune).

Ottimizza e misura gli strumenti

Dopo aver creato team specializzati per diversi domini di sicurezza, allinea i team tra loro. AWS Security Hub CSPMpuò aiutarti a raggiungere questo obiettivo. Security Hub CSPM offre una dashboard centralizzata e unificata per monitorare i progressi rispetto ai framework. Si integra inoltre con AWS i servizi di sicurezza molti strumenti di terze parti.

Il National Institute of Standards and Technology (NIST) Cybersecurity Framework sul sito web del NIST comprende cinque funzioni: identificazione, protezione, rilevamento, risposta e ripristino. L'immagine seguente mostra come utilizzare diversi Servizi AWS durante ogni funzione e quindi configurare tali servizi per inviare i risultati a Security Hub CSPM per la generazione di report consolidati. Se scegli di utilizzare altri strumenti, puoi utilizzare l'API CSPM di Security Hub, AWS Command Line Interface (AWS CLI) e AWS Security Finding Format (ASFF) per creare integrazioni personalizzate. Per ulteriori informazioni sulle integrazioni CSPM di Security Hub con altri servizi, consulta Integrazioni dei prodotti nella documentazione CSPM AWS Security Hub CSPM di Security Hub.



Security Hub CSPM si integra con tutti questi servizi e strumenti e fornisce quanto segue:

- Fornisce una dashboard unificata che mostra gli aggiornamenti e aiuta i team a eseguire le iterazioni sul posto
- Si integra automaticamente con i servizi AWS di sicurezza, come Amazon Macie, Amazon e GuardDutyAmazon Detective
- Supporta l'integrazione con strumenti di terze parti, come e Prowlercfn_nag
- Supporta integrazioni personalizzate con strumenti come l'API CSPM di Security Hub e il AWS Security Finding Format (ASFF) AWS CLI

Ottimizza e misura il rischio

Durante la fase matura della fase di camminata, puoi utilizzarla AWS Security Hub CSPM per ottimizzare e misurare continuamente il rischio per la sicurezza. Security Hub CSPM valuta continuamente il livello di sicurezza di un'organizzazione e intraprende azioni per risolvere i problemi identificati. Security Hub CSPM centralizza e dà priorità ai risultati di sicurezza provenienti da tutti i servizi e dai partner Account AWS terzi supportati. Ciò consente di analizzare le tendenze in materia di sicurezza e identificare i problemi di sicurezza ad alta priorità.

Security Hub CSPM esegue centinaia di controlli di sicurezza e li classifica in base al rischio per l'ambiente. AWS Puoi visualizzare il tuo punteggio rispetto ai controlli di sicurezza in una dashboard unificata nella console Security Hub CSPM. Per ulteriori informazioni, consulta Determinazione dei punteggi di sicurezza nella documentazione CSPM di Security Hub. Tramite questa dashboard, la DevSecOps funzione è in grado di identificare rapidamente eventuali controlli non riusciti, la gravità del problema di sicurezza Regione AWS e le risorse interessate. Una volta identificato, il DevSecOps team può stabilire le priorità e risolvere il problema. Man mano che i problemi vengono risolti, Security Hub CSPM aggiorna automaticamente lo stato.

Esamina esempi di casi d'uso nella fase matura

Di seguito sono riportati alcuni esempi della fase matura. Questi esempi approfondiscono i modelli, gli strumenti e i processi per i diversi obiettivi aziendali, a livello pratico.

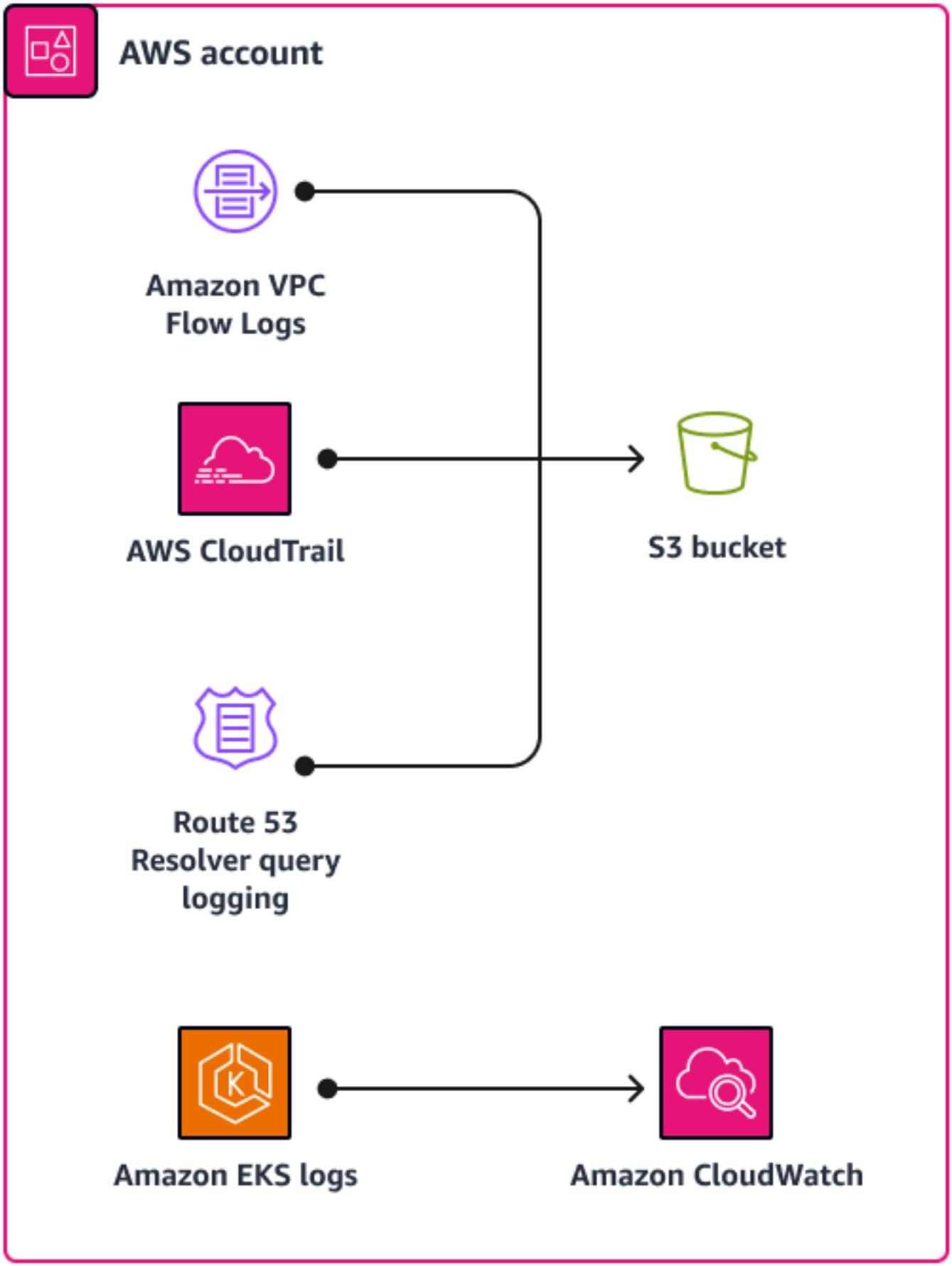
Maturo: esempio di rilevamento delle minacce

Risultato aziendale per i controlli investigativi: aumenta la visibilità e la velocità di rilevamento degli incidenti cloud per ridurre i rischi e consentire l'uso e lo sviluppo accelerati delle risorse cloud.

Tool: Assisted Log Enabler for AWS(GitHub) è uno strumento open source che consente di attivare la registrazione nel bel mezzo di un incidente di sicurezza. Può aumentare rapidamente la visibilità su un incidente.

Esempio di caso d'uso: si consideri il caso d'uso di un singolo account illustrato nel diagramma seguente. Vi sono eventi che richiedono ulteriori indagini. Non sei sicuro che la registrazione sia abilitata. In questo caso, la cosa migliore da fare è eseguire un dry run con the Assisted Log Enabler per vedere quali servizi sono abilitati o disabilitati. Assisted Log Enablerverifica la presenza di AWS CloudTrail percorsi, log di query DNS, log di flusso VPC e altri log. Se non sono abilitati, li abilita. Assisted Log Enabler Assisted Log Enablerpuò verificare e attivare la registrazione per tutti Regioni AWS.

Puoi anche accelerare verso l'alto o Assisted Log Enabler verso il basso. Dopo aver completato la corsa a secco, chiuso l'evento e risolto il problema, ti rendi conto che non hai più bisogno di questo livello di registrazione. È possibile ripulire rapidamente la distribuzione per interrompere la registrazione. Questa funzione consente di utilizzarla Assisted Log Enabler come strumento di triage.


AWS account
Amazon VPC Flow Logs
AWS CloudTrail
S3 bucket
Route 53 Resolver query logging
Amazon EKS logs
Amazon CloudWatch

Di seguito sono riportate le caratteristiche principali diAssisted Log Enabler for AWS:

- È possibile eseguirlo in un ambiente con account singolo o multiaccount.
- È possibile utilizzarlo per stabilire una linea di base per l'accesso al proprio ambiente.
- È possibile utilizzare la funzione dry run per verificare lo stato corrente e determinare quali servizi hanno la registrazione abilitata.
- È possibile selezionare i servizi per cui si desidera abilitare la registrazione.
- Puoi Assisted Log Enabler aumentare o diminuire la velocità, a seconda del tuo caso d'uso.

Maturo: esempio IAM

Risultato aziendale di IAM: automatizza la visibilità e utilizza misure basate sulle migliori pratiche per ridurre continuamente i rischi, abilitare connessioni esterne sicure e fornire rapidamente nuovi utenti e ambienti

Strumento:AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) ti aiuta a identificare le risorse condivise con un'entità esterna, convalida le politiche IAM rispetto alla grammatica e alle best practice delle policy e genera policy IAM basate sulle attività di accesso storiche. Ti consigliamo vivamente di abilitare IAM Access Analyzer sia a livello di account che di organizzazione.

Vantaggi del servizio: IAM Access Analyzer fornisce una vasta gamma di risultati approfonditi. Può identificare le risorse e gli account dell'organizzazione condivisi con un'entità esterna. Può rilevare risorse come un bucket S3 pubblico, un bucket AWS KMS key condiviso con un altro account o un ruolo condiviso con un account esterno, offrendoti un'eccellente visibilità sull'identificazione delle risorse che non sono sotto il controllo dell'organizzazione. Non solo convalida le policy IAM, ma può anche generarle per te.

Fase di esecuzione: ottimizzazione delle operazioni di sicurezza nel cloud

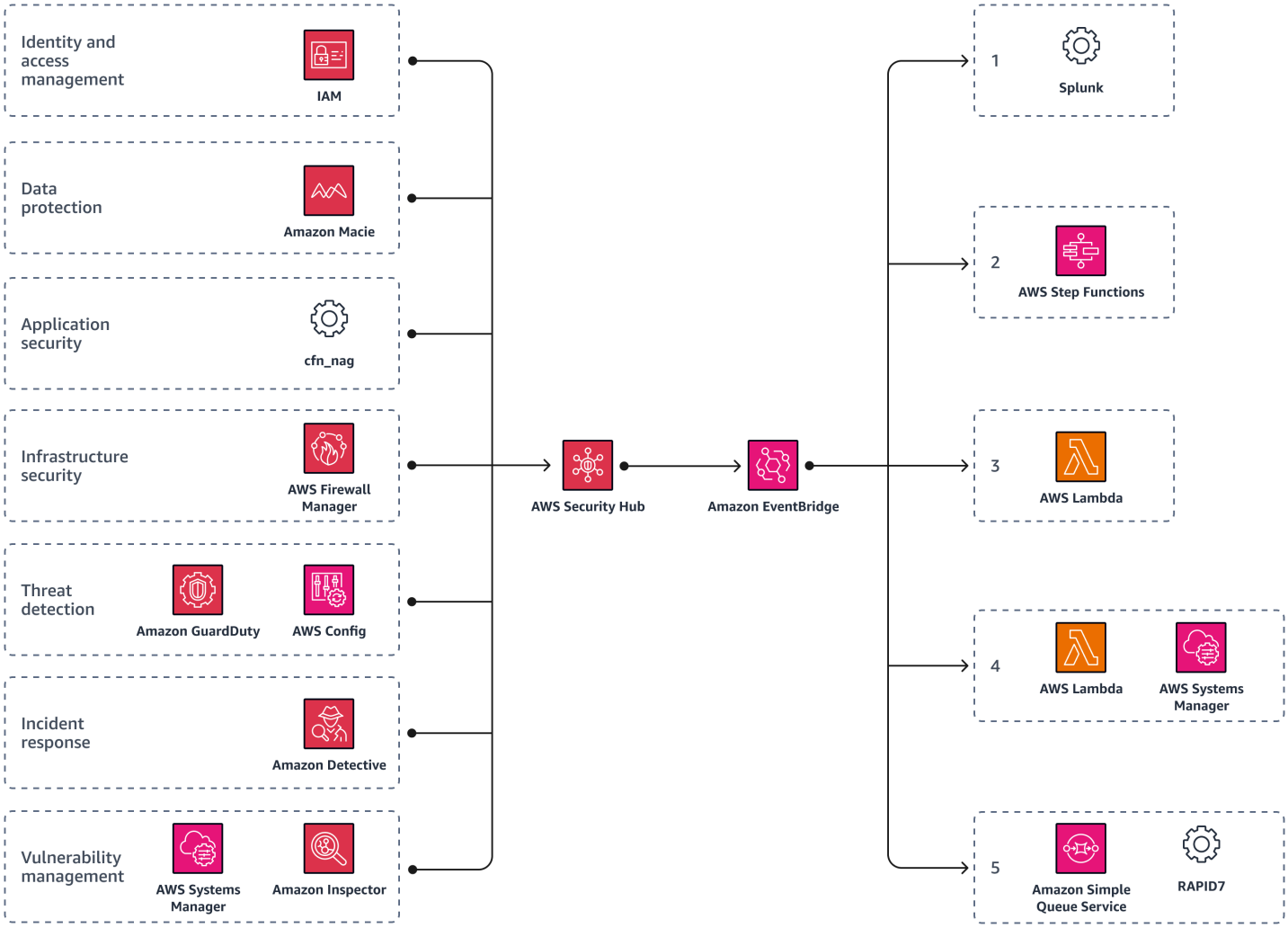
Dopo aver implementato una linea di base nella fase di camminata, l'organizzazione passa alla fase di corsa. Questa fase è incentrata sulla dimostrazione delle funzionalità di sicurezza informatica disponibili nel cloud, molte delle quali non sono possibili o sono molto difficili da implementare con soluzioni locali. Questa fase riunisce diversi componenti di sicurezza e automatizza i processi. Le automazioni liberano le risorse in modo che possano concentrarsi su lavori di alto valore.

La seguente è l'unica fase della fase di esecuzione:

- Ottimizza— Come posso migliorare questo processo e aggiungere l'automazione?

Ottimizzazione: automatizza e itera le tue operazioni di sicurezza sul cloud

Nella fase di ottimizzazione, automatizzi le tue operazioni di sicurezza. Come le fasi crawl e walk, è possibile utilizzarle AWS Security Hub CSPM durante la fase di esecuzione per ottenere l'automazione e l'iterazione. L'immagine seguente mostra come Security Hub CSPM può attivare una EventBridge regola Amazon personalizzata che definisce azioni automatiche da intraprendere in base a risultati e approfondimenti specifici. Per ulteriori informazioni, consulta Automazioni nella documentazione CSPM di Security Hub.



Utilizzando Security Hub CSPM come hub di automazione centrale, puoi anche inoltrare le attività a. Splunk Splunkpuò quindi rilevare quelle anomale e attivare le azioni corrispondenti in. EventBridge Ciò consente di automatizzare le attività ripetitive e offre più tempo ai membri del team qualificati per concentrarsi su attività di maggior valore. È inoltre possibile utilizzarlo AWS Step Functionsper raccogliere registri, scattare istantanee forensi, mettere in quarantena i server compromessi e sostituirli con un'immagine dorata. Inoltre, puoi utilizzare una AWS Lambdafunzione che consente di correggere le vulnerabilità nell'ambiente e utilizza una funzione Amazon Simple Queue Service (Amazon SQS) per convalidare la sicurezza dei sistemi. AWS Systems Manager Adottando questo approccio, è possibile contenere e porre rimedio rapidamente agli incidenti di sicurezza con un impatto minimo sulle normali operazioni aziendali.

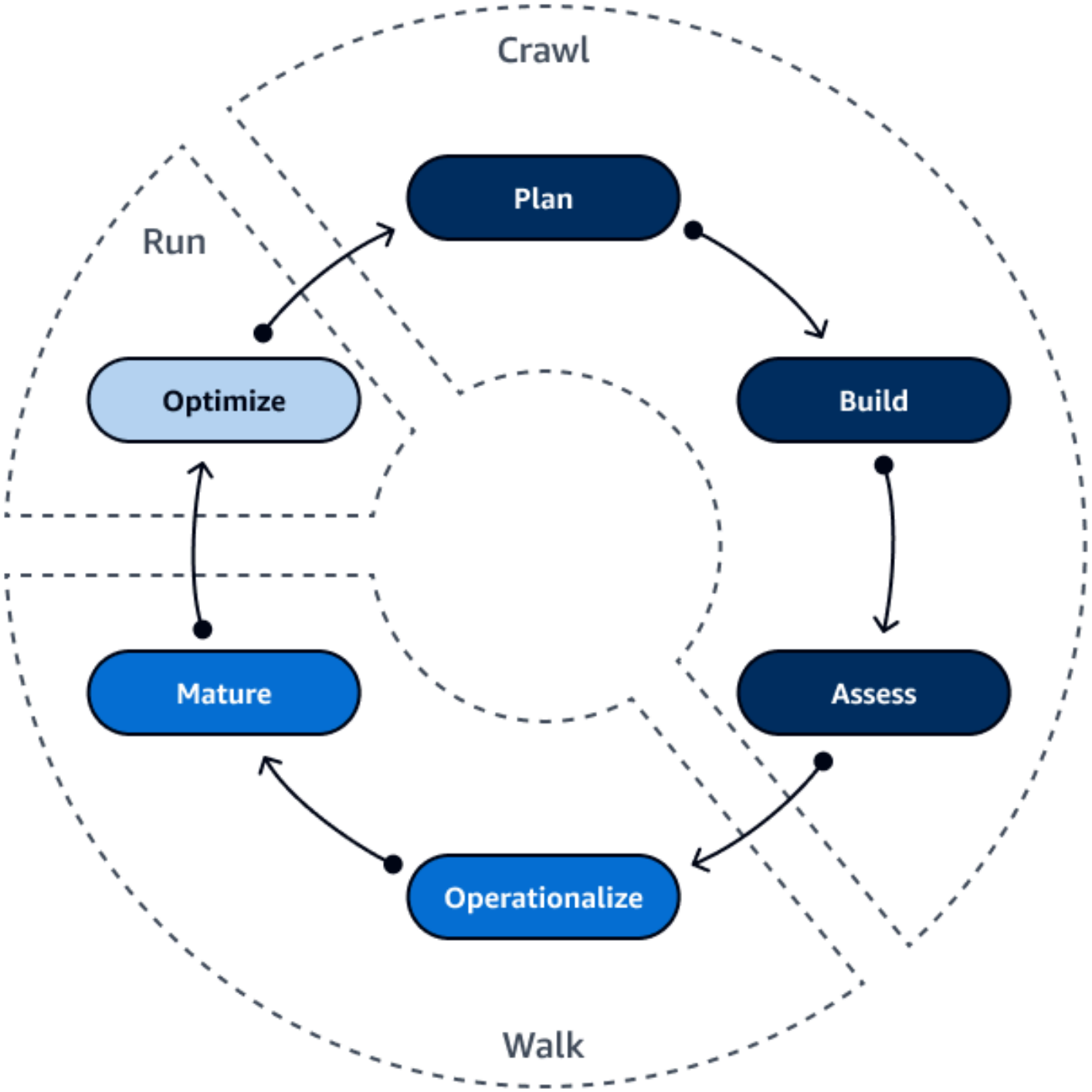
Di seguito è riportato un esempio di azioni automatizzate ripetute, come mostrato nell'immagine precedente:

1. SplunkDa utilizzare per rilevare attività discutibili.
2. Usa Step Functions per raccogliere registri, revocare l'accesso, mettere in quarantena e scattare istantanee forensi.
3. Usa una EventBridge regola per avviare una funzione Lambda che mette in quarantena, scatta istantanee forensi e sostituisce i server compromessi con un'immagine dorata.
4. Avvia una funzione Lambda che utilizza Systems Manager per correggere e applicare patch nel resto dell'ambiente.
5. Avvia un messaggio Amazon SQS che utilizza lo scanner Rapid7 per scansionare e verificare se la AWS risorsa è sicura.

Per ulteriori informazioni, consulta Come automatizzare la risposta agli incidenti Cloud AWS per le istanze EC2 nel Security Blog. AWS

Conclusione: gattona, cammina, corri, poi vola!

In sintesi, il modello crawl, walk, run è un framework che consente di migliorare gradualmente il livello di sicurezza e adottare le migliori pratiche per proteggere l'infrastruttura. AWS Questo processo continua a evolversi con l'emergere di nuove tecnologie ed esigenze aziendali. Seguendo questo framework e utilizzando le risorse fornite da AWS, è possibile stabilire una solida base per la sicurezza del cloud, gestire efficacemente i rischi di sicurezza, accelerare la maturità della sicurezza e promuovere l'innovazione.

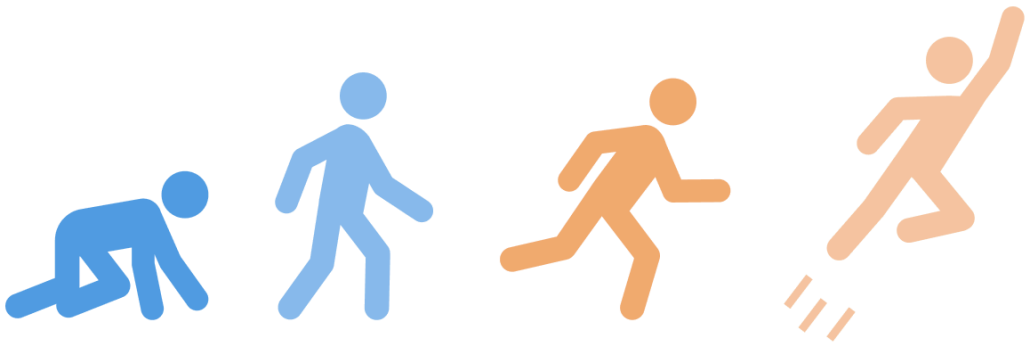


Nella fase di esplorazione, sei tu a porre le basi. Siete voi a definire il vostro piano di sicurezza, a utilizzare un'architettura di best practice di sicurezza definita e a condurre una valutazione continua degli obiettivi aziendali dell'organizzazione.

Nella fase di camminata, fai i primi passi. Analizzi le politiche, elabori schemi, formi le persone e allinei le strategie. Questa fase ti aiuta a capire come sfruttare l'innovazione per stare al passo con le tecnologie nel cloud.

Nella fase di corsa, si pensa in grande. Utilizzate l'automazione e posizionate strategicamente le vostre persone qualificate nel posto giusto. Implementate l'automazione per promuovere la valutazione continua verso gli obiettivi aziendali della vostra organizzazione.

Ora è il momento di volare. Utilizzate i consigli di questa guida per accelerare la maturità della sicurezza in. Cloud AWS



Risorse

Framework e modelli

- AWS Cloud Adoption Framework (CAF)AWS
- AWS Well-Architected Framework
- AWS Architettura di riferimento per la sicurezza (AWS SRA)
- AWS Modello di maturità della sicurezza
- Architettura di riferimento HIPAA
- Architettura di riferimento HITRUST

Servizi AWS

- AWS Control Tower
- AWS Identity and Access Management Access Analyzer
- AWS Security Hub CSPM

Altre risorse AWS

- Risposta di sicurezza automatizzata AWS attiva nella libreria AWS delle soluzioni
- Automatizza le tue operazioni IT utilizzando AWS Step Functions Amazon CloudWatch Events nel blog AWS Compute
- Come automatizzare la risposta agli incidenti nelle quattro Cloud AWS EC2 istanze del Security Blog AWS
- Come eseguire una risposta automatica agli incidenti in un ambiente con più account nel Security Blog AWS
- AWS Re:inForce 2022 - Crawl, walk, run: video sull'accelerazione della maturità in materia di sicurezza attivo YouTube
- AWS re:Inforce 2022 - Crawl, walk, run: presentazione accelerata della maturità in materia di sicurezza (allegato) PowerPoint

Collaboratori

Le seguenti persone hanno contribuito a questa guida.

Scrittura

- Chad Lorenc, responsabile delle pratiche di sicurezza, AWS
- Ivy Gin, consulente per la garanzia della sicurezza, AWS
- Sayali Paseband, consulente per la sicurezza, AWS

Revisione

- Deeps Baisya, architetto senior della sicurezza, AWS
- Mike LaRue, consulente senior per la sicurezza, AWS
- Raul Radu, ingegnere senior della sicurezza, AWS

Scrittura tecnica

- Lilly AbouHarb, scrittrice tecnica senior, AWS

Cronologia dei documenti

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

Modifica	Descrizione	Data
Pubblicazione iniziale	—	20 dicembre 2023

AWS Glossario delle linee guida prescrittive

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

Numeri

7 R

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

- Rifattorizzare/riprogettare: trasferisci un'applicazione e modifica la sua architettura sfruttando appieno le funzionalità native del cloud per migliorare l'agilità, le prestazioni e la scalabilità. Ciò comporta in genere la portabilità del sistema operativo e del database. Esempio: migra il tuo database Oracle locale all'edizione compatibile con Amazon Aurora PostgreSQL.
- Ridefinire la piattaforma (lift and reshape): trasferisci un'applicazione nel cloud e introduci un certo livello di ottimizzazione per sfruttare le funzionalità del cloud. Esempio: migra il tuo database Oracle locale ad Amazon Relational Database Service (Amazon RDS) per Oracle in. Cloud AWS
- Riacquistare (drop and shop): passa a un prodotto diverso, in genere effettuando la transizione da una licenza tradizionale a un modello SaaS. Esempio: migra il tuo sistema di gestione delle relazioni con i clienti (CRM) su Salesforce.com.
- Eseguire il rehosting (lift and shift): trasferisci un'applicazione sul cloud senza apportare modifiche per sfruttare le funzionalità del cloud. Esempio: migra il 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 del 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 di aggregazione

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 AIOps viene utilizzata nella strategia di AWS migrazione, consulta la guida all'integrazione delle operazioni.

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

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

AWS Workload Qualification Framework (WQF)AWS

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

B

bot difettoso

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

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

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

Classificazione binaria

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

filtro Bloom

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

implementazione blu/verde

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 Cloud Adoption AWS Framework.

implementazione canaria

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

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

Centro di eccellenza cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

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

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

CMDB

Vedi database di gestione della configurazione.

repository di codice

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

cache fredda

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

dati freddi

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

visione artificiale (CV)

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

deriva della configurazione

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

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

Il processo di automazione delle fasi di origine, compilazione, test, gestione temporanea e produzione del processo di rilascio del software. CI/CD viene comunemente descritto come una pipeline. CI/CD può aiutarvi ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le consegne. Per ulteriori informazioni, consulta Vantaggi

della distribuzione continua. CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta Distribuzione continua e implementazione continua a confronto.

CV

Vedi visione artificiale.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

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

deriva dei dati

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

dati in transito

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

rete di dati

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di definizione del database.

deep ensemble

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

deep learning

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

defense-in-depth

Un approccio alla sicurezza delle informazioni in cui una serie di meccanismi e controlli di sicurezza sono accuratamente stratificati su una rete di computer per proteggere la riservatezza, l'integrità e la disponibilità della rete e dei dati al suo interno. Quando si adotta questa strategia AWS, si aggiungono più controlli a diversi livelli della AWS Organizations struttura per proteggere le risorse. Ad esempio, un defense-in-depth approccio potrebbe combinare l'autenticazione a più fattori, la segmentazione della rete e la crittografia.

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

Un processo utilizzato per identificare e dare priorità ai vincoli che influiscono negativamente sulla velocità e sulla qualità nel ciclo di vita dello sviluppo del software. DVSM estende il processo di

mappatura del flusso di valore originariamente progettato per pratiche di produzione snella. Si concentra sulle fasi e sui team necessari per creare e trasferire valore attraverso il processo di sviluppo del software.

gemello digitale

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

tabella delle dimensioni

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

disastro

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

disaster recovery (DR)

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

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

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

DOTT.

Vedi disaster recovery.

rilevamento della deriva

Tracciamento delle deviazioni da una configurazione di base. Ad esempio, 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.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

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

scambio elettronico di dati (EDI)

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

crittografia

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

chiave crittografica

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

endianità

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

endpoint

Vedi service endpoint.

servizio endpoint

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

pianificazione delle risorse aziendali (ERP)

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

crittografia envelope

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

ambiente

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

- ambiente di sviluppo: un'istanza di un'applicazione in esecuzione disponibile solo per il team principale responsabile della manutenzione dell'applicazione. Gli ambienti di sviluppo vengono utilizzati per testare le modifiche prima di promuoverle negli ambienti superiori. Questo tipo di ambiente viene talvolta definito ambiente di test.
- ambienti inferiori: tutti gli ambienti di sviluppo di un'applicazione, ad esempio quelli utilizzati per le build e i test iniziali.

- ambiente di produzione: un'istanza di un'applicazione in esecuzione a cui gli utenti finali possono accedere. In una CI/CD pipeline, l'ambiente di produzione è l'ultimo ambiente di distribuzione.
- ambienti superiori: tutti gli ambienti a cui possono accedere utenti diversi dal team di sviluppo principale. Si può trattare di un ambiente di produzione, ambienti di preproduzione e ambienti per i test di accettazione da parte degli utenti.

epica

Nelle metodologie agili, categorie funzionali che aiutano a organizzare e dare priorità al lavoro. Le epiche forniscono una descrizione di alto livello dei requisiti e delle attività di implementazione. Ad esempio, le epopee della sicurezza AWS CAF includono la gestione delle identità e degli accessi, i controlli investigativi, la sicurezza dell'infrastruttura, la protezione dei dati e la risposta agli incidenti. Per ulteriori informazioni sulle epiche, consulta la strategia di migrazione AWS , consulta la guida all'implementazione del programma.

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

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

F

tabella dei fatti

Il tavolo centrale 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, consulta Interpretabilità del modello di machine learning con AWS.

trasformazione delle funzionalità

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

prompt con pochi scatti

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

Vedi modello di base.

modello di fondazione (FM)

Una grande rete neurale di deep learning che si è addestrata su enormi set di dati generalizzati e non etichettati. FMs sono in grado di svolgere un'ampia varietà di attività generali, come comprendere il linguaggio, generare testo e immagini e conversare in linguaggio naturale. Per ulteriori informazioni, consulta Cosa sono i modelli Foundation.

G

IA generativa

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

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

immagine dorata

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

strategia greenfield

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

guardrail

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

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

Migrazione del database di origine in un database di destinazione che utilizza un motore di database diverso (ad esempio, da Oracle ad Amazon Aurora). La migrazione eterogenea fa in

genere parte di uno sforzo di riprogettazione e la conversione dello schema può essere un'attività complessa. AWS offre AWS SCT che aiuta con le conversioni dello schema.

alta disponibilità (HA)

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

modernizzazione storica

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

dati di blocco

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

Subito dopo la conversione, il periodo di tempo in cui un team di migrazione gestisce e monitora le applicazioni migrate nel cloud per risolvere eventuali problemi. In genere, questo periodo dura

da 1 a 4 giorni. Al termine del periodo di hypercare, il team addetto alla migrazione in genere trasferisce la responsabilità delle applicazioni al team addetto alle operazioni cloud.

I

IaC

Vedi l'infrastruttura come codice.

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

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

VPC in ingresso (ingress)

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

migrazione incrementale

Una strategia di conversione in cui si esegue la migrazione dell'applicazione in piccole parti anziché eseguire una conversione singola e completa. Ad esempio, inizialmente potresti spostare

solo alcuni microservizi o utenti nel nuovo sistema. Dopo aver verificato che tutto funzioni correttamente, puoi spostare in modo incrementale microservizi o utenti aggiuntivi fino alla disattivazione del sistema legacy. Questa strategia riduce i rischi associati alle migrazioni di grandi dimensioni.

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

IIoInternet delle cose industriale (T)

L'uso di sensori e dispositivi connessi a Internet nei settori industriali, come quello manifatturiero, energetico, automobilistico, sanitario, delle scienze della vita e dell'agricoltura. Per ulteriori informazioni, vedere Creazione di una strategia di trasformazione digitale per l'Internet of Things (IIoT) industriale.

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

informazioni sulle zone di destinazione, consulta la sezione Configurazione di un ambiente AWS multi-account sicuro e scalabile.

modello linguistico di grandi dimensioni (LLM)

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

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

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

Un tipo di intelligenza artificiale che utilizza algoritmi e tecniche per il riconoscimento e l'apprendimento di schemi. Il machine learning analizza e apprende dai dati registrati, come i dati

dell'Internet delle cose (IoT), per generare un modello statistico basato su modelli. Per ulteriori informazioni, consulta la sezione Machine learning.

ramo principale

Vedi filiale.

malware

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

servizi gestiti

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

sistema di esecuzione della produzione (MES)

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

MAP

Vedi Migration Acceleration Program.

meccanismo

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

account membro

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

MEH

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

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

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

Un AWS programma che fornisce consulenza, supporto, formazione e servizi per aiutare le organizzazioni a costruire una solida base operativa per il passaggio al cloud e per contribuire a compensare il costo iniziale delle migrazioni. MAP include una metodologia di migrazione per eseguire le migrazioni precedenti in modo metodico e un set di strumenti per automatizzare e accelerare gli scenari di migrazione comuni.

migrazione su larga scala

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

fabbrica di migrazione

Team interfunzionali che semplificano la migrazione dei carichi di lavoro attraverso approcci automatizzati e agili. I team di Migration Factory in genere includono addetti alle operazioni,

analisti e proprietari aziendali, ingegneri addetti alla migrazione, sviluppatori e DevOps professionisti che lavorano nell'ambito degli sprint. Tra il 20% e il 50% di un portfolio di applicazioni aziendali è costituito da schemi ripetuti che possono essere ottimizzati con un approccio di fabbrica. Per ulteriori informazioni, consulta la discussione sulle fabbriche di migrazione e la Guida alla fabbrica di migrazione al cloud in questo set di contenuti.

metadati di migrazione

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

modello di migrazione

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

ORR

Vedi la revisione della prontezza operativa.

NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

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

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

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

persistenza poliglotta

Scelta indipendente della tecnologia di archiviazione di dati di un microservizio in base ai modelli di accesso ai dati e ad altri requisiti. Se i microservizi utilizzano la stessa tecnologia di archiviazione di dati, possono incontrare problemi di implementazione o registrare prestazioni scadenti. I microservizi vengono implementati più facilmente e ottengono prestazioni e scalabilità migliori se utilizzano l'archivio dati più adatto alle loro esigenze.

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

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

concatenamento rapido

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

pseudonimizzazione

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

publish/subscribe (pub/sub)

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

Q

Piano di query

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

regressione del piano di query

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

R

Matrice RACI

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

RAG

Vedi Retrieval Augmented Generation.

ransomware

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

Matrice RASCI

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

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

Region

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 alle interruzioni o di ripristinarle. L'elevata disponibilità e il disaster recovery sono considerazioni comuni quando si pianifica la resilienza in. Cloud AWSPer ulteriori informazioni, vedere Cloud AWS Resilience.

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi obiettivo del punto di ripristino.

VERSO

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

sicurezza fin dalla progettazione

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

Un'azione predefinita e programmata progettata per rispondere o porre rimedio automaticamente a un evento di sicurezza. Queste automazioni fungono da controlli di sicurezza investigativi o reattivi che aiutano a implementare le migliori pratiche di sicurezza. AWS Esempi di azioni di risposta automatizzate includono la modifica di un gruppo di sicurezza VPC, l'applicazione di patch a un'istanza 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 politica che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in. AWS Organizations SCPs definire barriere o fissare limiti alle azioni che un amministratore può delegare a utenti o ruoli. È possibile utilizzarli SCPs come elenchi consentiti o elenchi di rifiuto, per specificare quali servizi o azioni sono consentiti o proibiti. Per ulteriori informazioni, consulta le politiche di controllo del servizio nella AWS Organizations documentazione.

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

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

Modello di responsabilità condivisa

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

SIEM

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

punto di errore singolo (SPOF)

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

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

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

SPOF

Vedi punto di errore singolo.

schema a stella

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

modello del fico strangolatore

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

sottorete

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

controllo di supervisione e acquisizione dati (SCADA)

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

crittografia simmetrica

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

test sintetici

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

prompt di sistema

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

T

tag

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

variabile di destinazione

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

elenco di attività

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

ambiente di test

Vedi ambiente.

training

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

Transit Gateway

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

flusso di lavoro basato su trunk

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

Accesso attendibile

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

regolazione

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

team da due pizze

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

U

incertezza

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

compiti indifferenziati

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

ambienti superiori

Vedi ambiente.

V

vacuum

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

controllo delle versioni

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

Peering VPC

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

vulnerabilità

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

W

cache calda

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

dati caldi

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

funzione finestra

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

Carico di lavoro

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

flusso di lavoro

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

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

Z

exploit zero-day

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

vulnerabilità zero-day

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

prompt zero-shot

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

applicazione zombie

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

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