AWS Architettura di riferimento per la privacy (AWS PRA)

AWS Guida prescrittiva

AWS Guida prescrittiva: AWS Architettura di riferimento per la privacy (AWS PRA)

Table of Contents

AWS Architettura di riferimento per la privacy (AWS PRA)

Amazon Web Services (collaboratori)

Marzo 2024 (cronologia dei documenti)

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Note

Questa guida viene fornita solo a scopo informativo. Non è una consulenza legale e non dovrebbe essere considerata una consulenza legale. AWS incoraggia i propri clienti a ottenere una consulenza adeguata sull'implementazione degli ambienti di protezione della privacy e dei dati e, più in generale, sulle leggi applicabili alla loro attività.

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di AWS prodotto, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o assicurazione da parte AWS delle sue affiliate, fornitori o licenzianti. AWS i prodotti o i servizi sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite.

Le responsabilità e le responsabilità dei AWS propri clienti sono regolate da AWS accordi e il presente documento non fa parte di, né modifica, alcun accordo tra AWS e i suoi clienti.

Introduzione

La AWS Privacy Reference Architecture (PRA) fornisce una serie di linee guida specifiche per la progettazione e la configurazione dei controlli a supporto della privacy in. Servizi AWS Questa guida può aiutarti a prendere decisioni su persone, processi e tecnologie che aiutano a supportare la privacy in. Cloud AWS

Il modello di responsabilità AWS condivisa e la privacy

Nel Cloud AWS, condividi la responsabilità per la sicurezza e la conformità con AWS. AWS è responsabile della sicurezza del cloud, il che significa che AWS è responsabile della protezione

dell'infrastruttura che gestisce tutti i servizi offerti in Cloud AWS. L'utente è responsabile della sicurezza nel cloud, il che significa che è responsabile della configurazione e della gestione Servizi AWS in conformità ai requisiti di sicurezza e privacy. Per ulteriori informazioni, consulta il modello di responsabilitàAWS condivisa.

Servizi AWS forniscono funzionalità che consentono di implementare i propri controlli sulla privacy nel cloud per supportare i requisiti di privacy. La responsabilità dell'utente in materia di privacy varia in base a molti fattori, tra cui la Servizi AWS scelta dell' Regioni AWS utente, l'integrazione di tali servizi nell'ambiente IT e le leggi e i regolamenti applicabili all'organizzazione e al carico di lavoro.

Durante l'utilizzo Servizi AWS, mantieni il controllo sui tuoi contenuti. In particolare, per contenuti si intendono software (incluse le immagini automatiche), dati, testo, audio, video o immagini che l'utente o qualsiasi utente finale ci trasferisce per l'elaborazione, l'archiviazione o l'hosting Servizi AWS in relazione al proprio account. Include anche tutti i risultati computazionali ottenuti dall'utente o da un utente finale utilizzando. Servizi AWS L'utente è responsabile della gestione delle seguenti decisioni, che sono sotto il suo controllo:

- I dati su cui scegli di raccogliere, archiviare o elaborare AWS
- I dati Servizi AWS che usi con i dati
- Il Regione AWS luogo in cui raccogli, archivia o elabora i dati
- Il formato e la struttura dei dati e se sono mascherati, anonimi o crittografati
- Come definire, archiviare, ruotare e utilizzare le chiavi crittografiche per la crittografia
- Chi ha accesso e quando ha accesso ai tuoi dati e come tali diritti di accesso vengono concessi, gestiti e revocati

Una volta compreso il modello di responsabilità AWS condivisa e come si applica generalmente all'operatività nel cloud, è necessario determinare come si applica al proprio caso d'uso. Le opzioni Servizi AWS che scegli di utilizzare determinano la quantità di configurazione da eseguire nell'ambito delle responsabilità in materia di privacy dell'organizzazione. Ad esempio, un servizio come Amazon Elastic Compute Cloud (Amazon EC2) è classificato come infrastruttura come servizio (IaaS). Pertanto, se utilizzi Amazon EC2, devi eseguire tutte le configurazioni di privacy necessarie per i sistemi operativi guest e per il software applicativo o le utilità che installi sulle tue EC2 istanze. Quando si utilizza un servizio astratto, come Amazon Simple Storage Service (Amazon S3) e Amazon DynamoDB AWS , è responsabile del livello di infrastruttura, del sistema operativo e delle piattaforme. La tua responsabilità è gestire e classificare i dati e configurare le politiche utilizzate per

accedere agli endpoint al fine di archiviare e recuperare i dati. Per ulteriori informazioni su come AWS proteggere i dati e la privacy, consulta Protezione dei dati e privacy all'indirizzo. AWS

Comprendere il AWS PRA

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

La sezione descrive la relazione tra la AWS Privacy Reference Architecture (AWS PRA) e altre AWS linee guida. Questa sezione esamina anche il layout e la struttura generali dell'ambiente AWS multi-account di esempio nel AWS PRA.

Questa sezione contiene i seguenti argomenti:

- Utilizzo del AWS PRA e dell' AWS SRA
- AWS Organizations e la struttura degli account dedicata
- Rendere operativi AWS i servizi per la privacy

Utilizzo del AWS PRA e dell' AWS SRA

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Il AWS PRA fornisce modelli che i clienti hanno trovato utili per pianificare controlli della privacy di base e a livello di applicazione per la loro infrastruttura e i loro carichi di lavoro. AWS La AWS Security Reference Architecture (AWS SRA) fornisce una serie di linee guida per la creazione di un'architettura che implementa e supporti il giusto set di controlli di sicurezza nella AWS landing zone e nelle applicazioni. Per stabilire i controlli sulla privacy descritti in questa guida, il AWS PRA si basa su molte delle stesse linee guida fondamentali e sulla stessa struttura degli account descritte nella SRA. AWS Il AWS PRA e l' AWS SRA descrivono molte delle stesse chiavi. Servizi AWS Questa guida include solo brevi descrizioni di questi servizi. Puoi saperne di più su questi servizi e su come vengono utilizzati in un contesto di sicurezza nell' AWS SRA.

L' AWS SRA può aiutarvi a progettare, implementare e gestire i servizi di AWS sicurezza in modo che siano in linea con AWS le pratiche consigliate. È possibile utilizzare la AWS SRA come guida autonoma oppure la AWS SRA e AWS la PRA come guide complementari. Molte delle linee guida di

sicurezza dettagliate nell' AWS SRA possono essere seguite insieme ai controlli sulla privacy descritti nel PRA. AWS Analogamente alla sicurezza, esistono considerazioni fondamentali sulla privacy che possono essere utili da prendere nelle prime fasi del Cloud AWS percorso, poiché queste decisioni possono influire sulla progettazione della struttura degli account dell'organizzazione. Ad esempio, alcune domande che potresti prendere in considerazione includono:

- In che modo la mia organizzazione definisce i dati personali?
- La mia organizzazione supporta applicazioni che trattano dati personali?
- Che dire delle applicazioni che elaborano altri tipi di dati regolamentati?
- Quali controlli a livello di organizzazione posso implementare per tenere i miei sviluppatori e ingegneri del cloud il più lontano possibile dai dati personali?
- Come faccio a separare i dati personali da altri tipi di dati?
- Quali sono i requisiti per il trasferimento transfrontaliero dei dati della mia organizzazione?

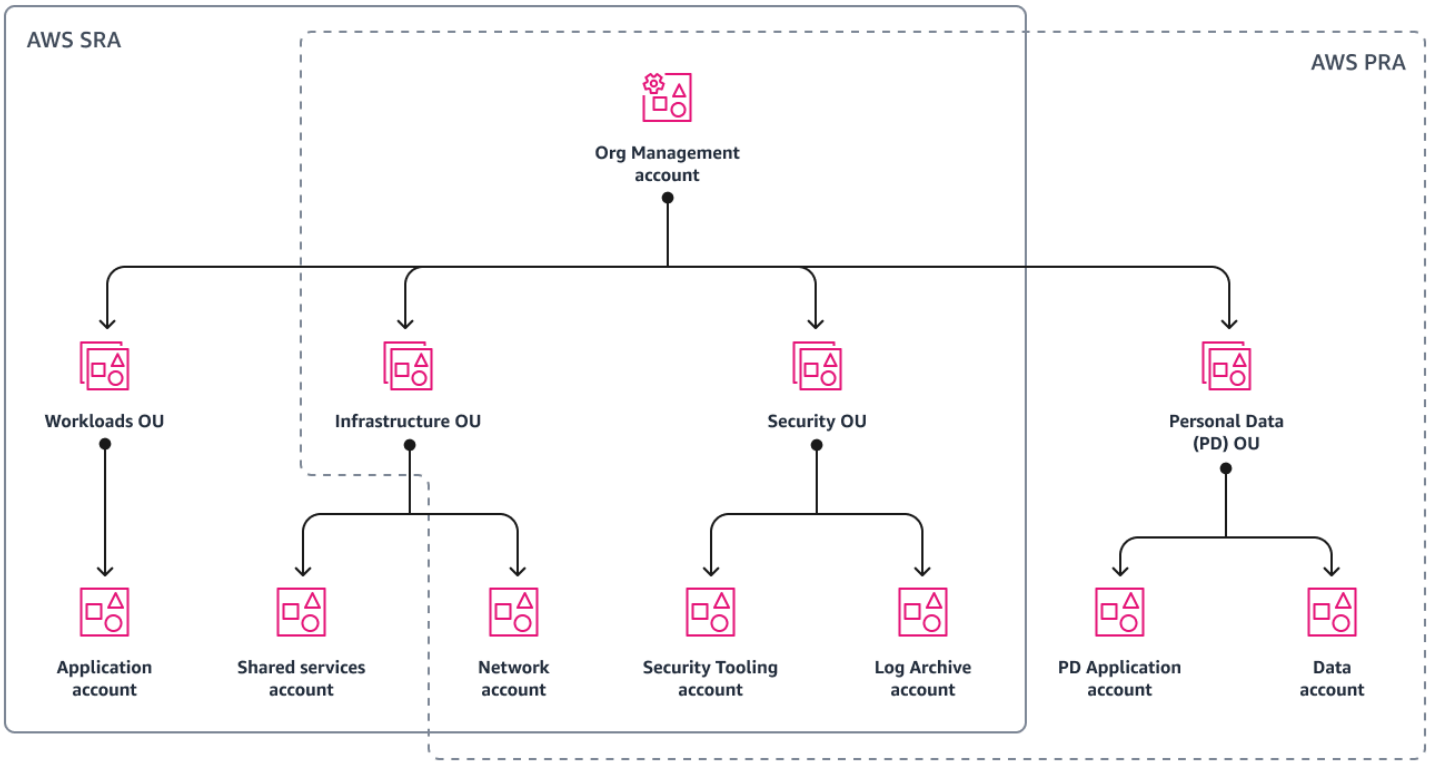
Le risposte a molte di queste domande possono avere implicazioni per la progettazione del tuo ambiente cloud, come la Account AWS struttura, le politiche di controllo dei servizi e i ruoli AWS Identity and Access Management (IAM).

AWS Organizations e la struttura degli account dedicata

> Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

AWS Organizationsè un servizio di gestione degli account che consente di gestire e amministrare centralmente più Account AWS account. L'uso di AWS Organizations è alla base di un ambiente multi-account ben progettato. AWS Per ulteriori informazioni, consulta Stabilire un ambiente basato sulle migliori pratiche. AWS

Il diagramma seguente mostra la struttura di account e unità organizzative (OU) di alto livello del AWS PRA. Per la maggior parte, la struttura organizzativa del AWS PRA corrisponde alla struttura organizzativa della AWS SRA.



Le deviazioni dall'organizzazione AWS SRA includono:

- Il AWS PRA aggiunge l'OU Personal Data (PD), dedicata alla raccolta, all'archiviazione e all'elaborazione dei dati personali. Questa separazione strutturale offre flessibilità in modo da poter definire controlli specifici e dettagliati per proteggere i dati personali dalla divulgazione involontaria.
- Nell'unità organizzativa Infrastructure, il AWS PRA attualmente non include indicazioni aggiuntive per l'account Shared Services descritto nell'SRA. AWS
- Attualmente la AWS PRA non include linee guida aggiuntive per l'unità organizzativa Workloads descritta nell' AWS SRA. Le applicazioni che raccolgono o trattano dati personali si trovano in account dedicati nell'unità organizzativa PD.

È possibile utilizzarle AWS Control Towerper la governance generale di base e l'implementazione automatizzata dei controlli di sicurezza e privacy in tutta l'organizzazione. Se AWS Control Tower non è attualmente in uso nell'organizzazione, è comunque possibile implementare molti dei controlli di sicurezza e privacy previsti AWS Control Tower, come le politiche e le AWS Config regole di controllo dei servizi, nei rispettivi servizi.

Potresti trovare utile prendere in considerazione il trattamento dei dati personali quando pianifichi il tuo account e la struttura delle unità organizzative, inclusa una strategia di segmentazione

dell'account. Potresti dover considerare i tipi di dati che stai trattando per i loro casi d'uso unici e per le leggi e i regolamenti applicabili. Ad esempio, i dati dei titolari di carta sono protetti dal Payment Card Industry Data Security Standard (PCI DSS) e le informazioni sanitarie protette potrebbero essere soggette all'Health Insurance Portability and Accountability Act (HIPAA). Potresti voler esaminare quali ambienti contengono dati personali e pianificare la tua strategia di segmentazione in modo approfondito su questi aspetti. Una tipica strategia di segmentazione degli account può includere account dedicati Account AWS che si adattano al ciclo di vita dello sviluppo del software (SDLC), ad esempio account dedicati allo sviluppo, alla gestione temporanea o al controllo della qualità (QA) e alla produzione. Una strategia di segmentazione come questa può essere un elemento fondamentale nella discussione generale sulla progettazione e OUs potrebbe essere necessario adeguarla ai requisiti normativi specifici.

Rendere operativi AWS i servizi per la privacy

> Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Per molti, la privacy è trasversale. Molti team diversi hanno un ruolo da svolgere, compresi i team addetti alla regolamentazione, alla conformità e agli ingegneri. Una volta che l'organizzazione ha iniziato a definire le persone e le componenti politiche chiave del programma sulla privacy, è possibile mappare i controlli rispetto a un framework di conformità alla privacy per operazioni coerenti. Un framework può fungere da rubrica per l'implementazione di controlli di privacy di base e specifici dell'applicazione per i dati personali nell'ambiente in uso. AWS

Indipendentemente dal framework utilizzato dai clienti per classificare i propri requisiti di privacy, i team addetti alla conformità alla privacy, all'ingegneria della privacy e alle applicazioni spesso devono collaborare per raggiungere gli obiettivi di implementazione. Ad esempio, i team addetti alla regolamentazione e alla conformità potrebbero fornire requisiti di alto livello e i team di progettazione e applicazione configurazioni Servizi AWS e funzionalità in base a tali requisiti. Partire da un framework di controllo può aiutarvi a definire controlli organizzativi e tecnici più prescrittivi.

Quando si definiscono i controlli tecnici Servizi AWS e le funzionalità, un'altra decisione chiave è se un controllo debba applicarsi all'intera organizzazione, a un'unità organizzativa, a un account o a una risorsa specifica. Alcuni servizi e funzionalità si adattano perfettamente all'implementazione dei controlli nell'intera AWS organizzazione. Ad esempio, il blocco dell'accesso pubblico ai bucket Amazon S3 è un controllo specifico che è preferibilmente configurato nella radice dell'organizzazione

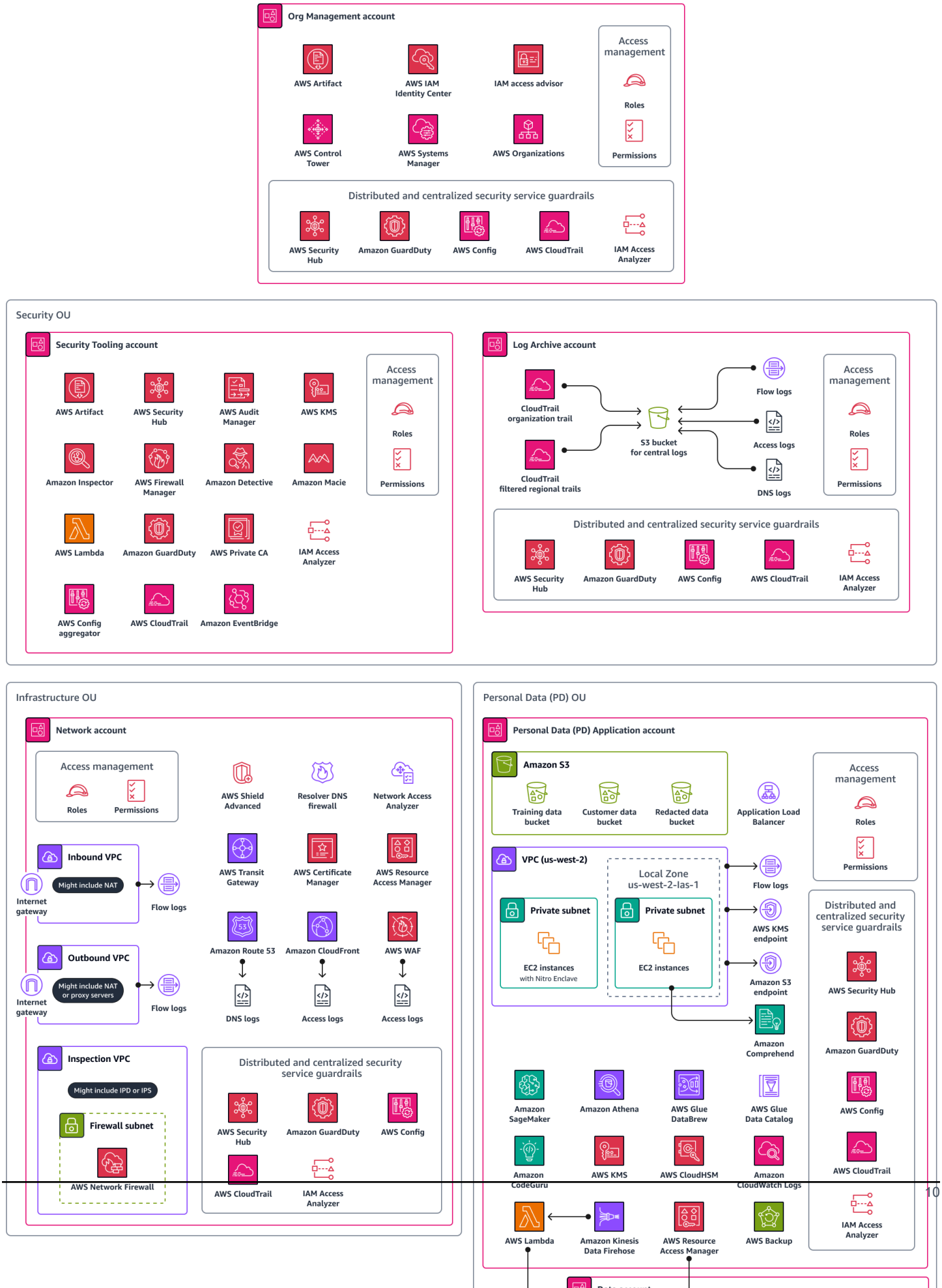
piuttosto che individualmente per ogni account. Tuttavia, le politiche di conservazione possono variare da un'applicazione all'altra, il che significa che è possibile applicare il controllo a livello di risorsa.

Per aiutarvi ad accelerare l'operazionalizzazione della privacy nella vostra organizzazione, AWS offre servizi di consulenza in materia di audit e conformità per i vostri carichi di lavoro. AWS Per ulteriori informazioni, contatta SAS. AWS

L'architettura di riferimento per la AWS privacy

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Il diagramma seguente illustra la AWS Privacy Reference Architecture (AWS PRA). Questo è un esempio di architettura che collega molte funzionalità e relative alla privacy Servizi AWS . Questa architettura è costruita su una landing zone governata da AWS Control Tower.


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
AWS Control Tower
AWS Systems Manager
AWS Organizations
Access management
Roles
Permissions
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
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
AWS Lambda
Amazon GuardDuty
AWS Private CA
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Access management
Roles
Permissions
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Personal Data (PD) OU
Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application Load Balancer
VPC (us-west-2)
Local Zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Amazon Comprehend
Amazon SageMaker
Amazon Athena
AWS Glue DataBrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Il AWS PRA include un'architettura web serverless ospitata nell'account dell'applicazione Personal Data (PD). L'architettura di questo account è un esempio di carico di lavoro che raccoglie dati personali direttamente dai consumatori. In questo carico di lavoro, gli utenti si connettono tramite un livello Web. Il livello web interagisce con il livello dell'applicazione. Questo livello riceve input dal livello Web, elabora e archivia i dati, consente ai team interni autorizzati e a terze parti di accedere ai dati e infine archivia ed elimina i dati quando non sono più necessari. L'architettura è volutamente modulare e basata sugli eventi per dimostrare molte delle tecniche fondamentali di ingegneria della privacy senza approfondire casi d'uso specifici, come data lake, contenitori, elaborazione o Internet of Things (IoT).

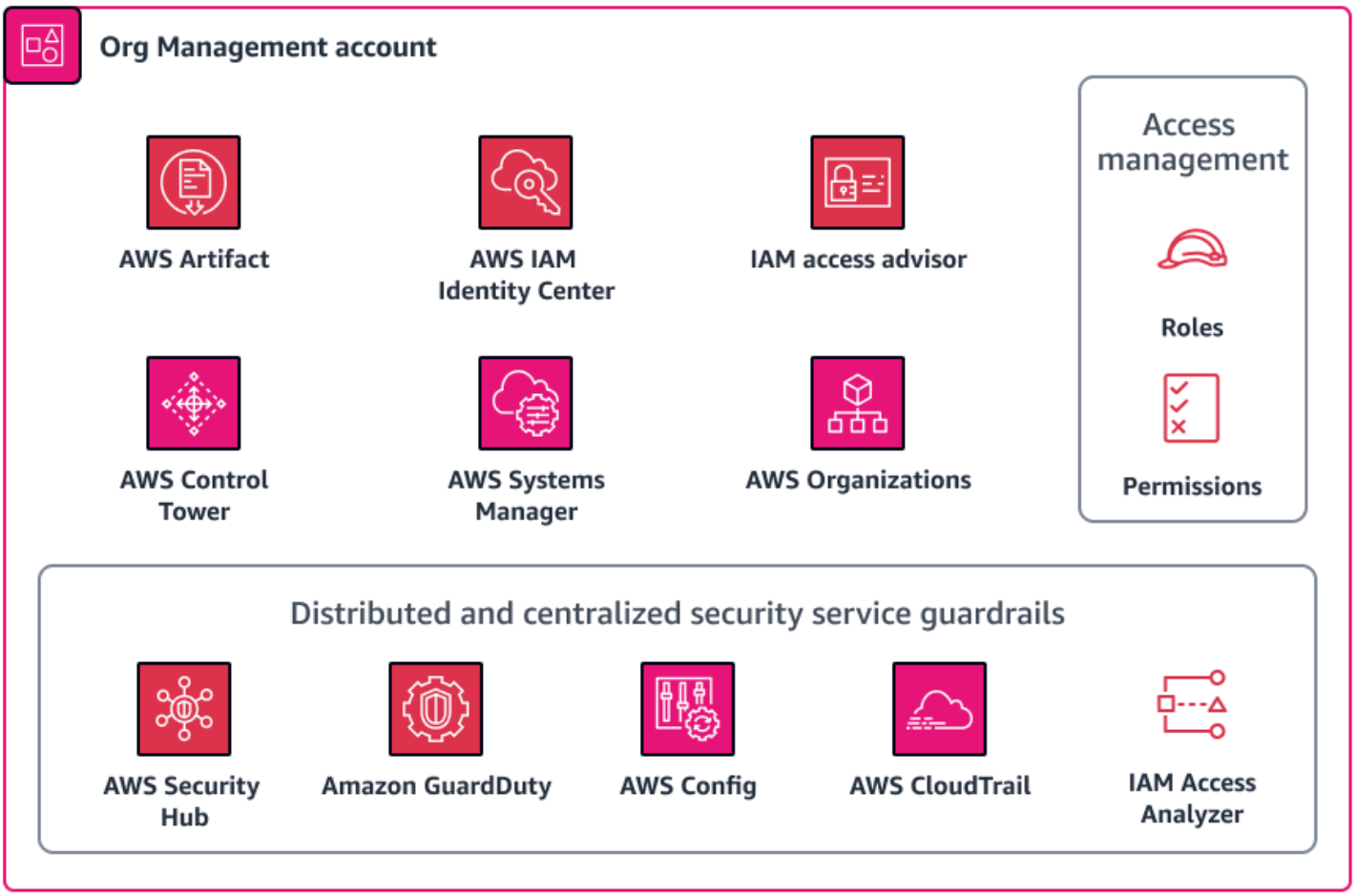
Successivamente, questa guida descrive in dettaglio ogni account dell'organizzazione. Descrive i servizi e le funzionalità relativi alla privacy, le considerazioni e i consigli e i diagrammi per ciascuno dei seguenti account:

- Account di gestione dell'organizzazione
- Security OU — Account Security Tooling
- Security OU: account Log Archive
- UO dell'infrastruttura - Account di rete
- Dati personali OU — Account dell'applicazione PD

Account di gestione dell'organizzazione

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

L'account Org Management viene utilizzato principalmente per gestire la modifica della configurazione delle risorse per i controlli di base sulla privacy di tutti gli account dell'organizzazione, che è gestita da. AWS Organizations Questo account è anche il luogo in cui è possibile implementare nuovi account membro in modo coerente, con molti degli stessi controlli di sicurezza e privacy. Per ulteriori informazioni su questo account, consulta la AWS Security Reference Architecture (AWS SRA). Il diagramma seguente illustra i servizi AWS di sicurezza e privacy configurati nell'account Org Management.



Questa sezione fornisce informazioni più dettagliate sui seguenti elementi Servizi AWS utilizzati in questo account:

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifactpuò aiutarvi con gli audit fornendo download su richiesta di documenti di AWS sicurezza e conformità. Per ulteriori informazioni su come questo servizio viene utilizzato in un contesto di sicurezza, consulta la AWS Security Reference Architecture.

In questo modo è possibile Servizio AWS comprendere i controlli da cui si eredita AWS e determinare quali controlli potrebbero rimanere da implementare nel proprio ambiente. AWS Artifact fornisce l'accesso ai report AWS di sicurezza e conformità, come i report SOC (System and Organization

Controls) e i report del settore delle carte di pagamento (PCI). Fornisce inoltre l'accesso alle certificazioni degli organismi di accreditamento di tutte le aree geografiche e dei verticali di conformità che convalidano l'implementazione e l'efficacia operativa dei controlli. AWS In pratica AWS Artifact, potete fornire gli elementi di AWS controllo ai revisori o alle autorità di regolamentazione come prova dei controlli di sicurezza. AWS I seguenti report potrebbero essere utili per dimostrare l'efficacia dei controlli sulla privacy: AWS

- Report sulla privacy SOC 2 Tipo 2: questo rapporto dimostra l'efficacia dei AWS controlli sul modo in cui i dati personali vengono raccolti, utilizzati, conservati, divulgati ed eliminati. Per ulteriori informazioni, consulta le domande frequenti su SOC.
- Rapporto sulla privacy SOC 3 — Il rapporto sulla privacy SOC 3 è una descrizione meno dettagliata dei controlli sulla privacy del SOC, per una diffusione generale.
- Rapporto di certificazione ISO/IEC 27701:2019 — ISO/IEC 27701:2019 descrive i requisiti e le linee guida per stabilire e migliorare continuamente un sistema di gestione delle informazioni sulla privacy (PIMS). Questo rapporto descrive in dettaglio l'ambito di questa certificazione e può fungere da prova della certificazione. AWS Per ulteriori informazioni su questo standard, vedere ISO/IEC 27701:2019 (sito web ISO).

AWS Control Tower

AWS Control Towerti aiuta a configurare e gestire un ambiente AWS multi-account che segue le migliori pratiche di sicurezza prescrittive. Per ulteriori informazioni su come questo servizio viene utilizzato in un contesto di sicurezza, consulta la Security Reference Architecture.AWS

Inoltre AWS Control Tower, puoi automatizzare l'implementazione di una serie di controlli proattivi, preventivi e investigativi, noti anche come guardrail, che si allineano ai requisiti di residenza e protezione dei dati. Ad esempio, puoi specificare dei guardrail che limitano il trasferimento dei dati ai soli dati approvati. Regioni AWSPer un controllo ancora più granulare, puoi scegliere tra più di 17 guardrail progettati per controllare la residenza dei dati, come Impedire connessioni Amazon Virtual Private Network (VPN), Impedire l'accesso a Internet per un'istanza Amazon VPC e Deny access a in base alla richiesta. AWS Regione AWS Questi guardrail sono costituiti da una serie di AWS CloudFormation hook, politiche di controllo dei servizi e regole che possono essere distribuiti in modo uniforme in tutta l'organizzazione. AWS Config Per ulteriori informazioni, consulta Controlli che migliorano la protezione della residenza dei dati nella documentazione. AWS Control Tower

Se è necessario implementare protezioni alla privacy oltre ai controlli sulla residenza dei dati, AWS Control Tower include una serie di controlli obbligatori. Questi controlli vengono implementati per

impostazione predefinita in tutte le unità organizzative quando configuri la landing zone. Molti di questi sono controlli preventivi progettati per proteggere i log, come Disallow Deletion of Log Archive e Enable Integrity Validation for Log File. CloudTrail

AWS Control Tower è inoltre integrato con AWS Security Hub per fornire controlli investigativi. Questi controlli sono noti come Service-Managed Standard:. AWS Control Tower Puoi utilizzare questi controlli per monitorare eventuali variazioni di configurazione dei controlli che supportano la privacy, come la crittografia a riposo per le istanze di database Amazon Relational Database Service (Amazon RDS).

AWS Organizations

Il AWS PRA gestisce centralmente tutti gli account AWS Organizations all'interno dell'architettura. Per ulteriori informazioni sul tagging, consulta AWS Organizations e la struttura degli account dedicatain questa guida. Nel AWS Organizations, puoi utilizzare le politiche di controllo del servizio (SCPs) e le politiche di gestione per proteggere i dati personali e la privacy.

Politiche di controllo del servizio (SCPs)

Le politiche di controllo del servizio (SCPs) sono un tipo di politica organizzativa che è possibile utilizzare per gestire le autorizzazioni all'interno dell'organizzazione. Forniscono il controllo centralizzato sulle autorizzazioni massime disponibili per i ruoli e gli utenti AWS Identity and Access Management (IAM) nell'account di destinazione, nell'unità organizzativa (OU) o nell'intera organizzazione. Puoi creare e candidarti SCPs dall'account di gestione dell'organizzazione.

Puoi utilizzarlo AWS Control Tower per distribuirlo in modo SCPs uniforme su tutti i tuoi account. Per ulteriori informazioni sui controlli di residenza dei dati che puoi utilizzare AWS Control Tower, consulta questa guidaAWS Control Tower. AWS Control Tower include una serie completa di misure preventive SCPs. Se AWS Control Tower non è attualmente utilizzato nella tua organizzazione, puoi anche distribuire questi controlli manualmente.

Utilizzato SCPs per soddisfare i requisiti di residenza dei dati

È comune gestire i requisiti di residenza dei dati personali archiviando ed elaborando i dati all'interno di un'area geografica specifica. Per verificare che i requisiti unici di residenza dei dati di una giurisdizione siano soddisfatti, ti consigliamo di lavorare a stretto contatto con il tuo team di regolamentazione per confermare i requisiti. Una volta determinati questi requisiti, esistono una serie di controlli di AWS base sulla privacy che possono aiutare a fornire assistenza. Ad esempio, è possibile utilizzare SCPs per limitare ciò che Regioni AWS può essere utilizzato per elaborare e

archiviare i dati. Per un esempio di politica, Limita i trasferimenti di dati tra Regioni AWS consulta questa guida.

Utilizzo SCPs per limitare le chiamate API ad alto rischio

È importante capire di quali controlli di sicurezza e privacy AWS è responsabile e di quali l'utente è responsabile. Ad esempio, sei responsabile dei risultati delle chiamate API che potrebbero essere effettuate rispetto a Servizi AWS quella che utilizzi. È inoltre tua responsabilità comprendere quali di queste chiamate potrebbero comportare modifiche al tuo atteggiamento in materia di sicurezza o privacy. Se sei preoccupato di mantenere un determinato livello di sicurezza e privacy, puoi abilitare SCPs questa opzione per negare determinate chiamate API. Queste chiamate API possono avere implicazioni, come la divulgazione involontaria di dati personali o le violazioni di specifici trasferimenti transfrontalieri di dati. Ad esempio, potresti voler vietare le seguenti chiamate API:

- Abilitazione dell'accesso pubblico ai bucket Amazon Simple Storage Service (Amazon S3)
- Disabilitazione di Amazon GuardDuty o creazione di regole di soppressione per i risultati dell'esfiltrazione di dati, come Trojan:/Exfiltration finding EC2 DNSData
- AWS WAF Eliminazione delle regole di esfiltrazione dei dati
- Condivisione pubblica degli snapshot di Amazon Elastic Block Store (Amazon EBS)
- Rimozione di un account membro dall'organizzazione
- Dissociazione di Amazon CodeGuru Reviewer da un repository

Politiche di gestione

Le politiche di gestione AWS Organizations possono aiutarti a configurare e gestire centralmente Servizi AWS e le relative funzionalità. I tipi di policy di gestione scelti determinano in che modo le politiche influiscono sugli account che li ereditano OUs e sugli account che li ereditano. Le politiche relative ai tag sono un esempio di politica di gestione in quanto AWS Organizations si riferisce direttamente alla privacy.

Utilizzo delle politiche relative ai tag

I tag sono coppie di valori chiave che consentono di gestire, identificare, organizzare, cercare e filtrare AWS le risorse. Può essere utile applicare tag che distinguano le risorse dell'organizzazione che gestiscono i dati personali. L'uso dei tag supporta molte delle soluzioni di privacy illustrate in questa guida. Ad esempio, potresti voler applicare un tag che indichi la classificazione generale dei dati elaborati o archiviati all'interno della risorsa. È possibile scrivere politiche di controllo degli accessi basate sugli attributi (ABAC) che limitano l'accesso alle risorse con un particolare tag o set

di tag. Ad esempio, la tua politica potrebbe specificare che il `SysAdmin` ruolo non può accedere alle risorse che hanno il tag. `dataclassification:4` Per ulteriori informazioni e un tutorial, consulta Definire le autorizzazioni per accedere alle AWS risorse in base ai tag nella documentazione IAM. Inoltre, se l'organizzazione utilizza l'applicazione generalizzata delle politiche di conservazione dei dati AWS Backupa tutti i backup di molti account, è possibile applicare un tag che inserisca tale risorsa nell'ambito di tale policy di backup.

Le politiche relative ai tag consentono di mantenere tag coerenti in tutta l'organizzazione. In una politica sui tag, specifichi le regole che si applicano alle risorse quando vengono etichettate. Ad esempio, puoi richiedere che le risorse siano etichettate con chiavi specifiche, come `DataClassification` o`DataSteward`, e puoi specificare casi o valori validi per le chiavi. È inoltre possibile utilizzare l'imposizione per impedire il completamento delle richieste di etichettatura non conformi.

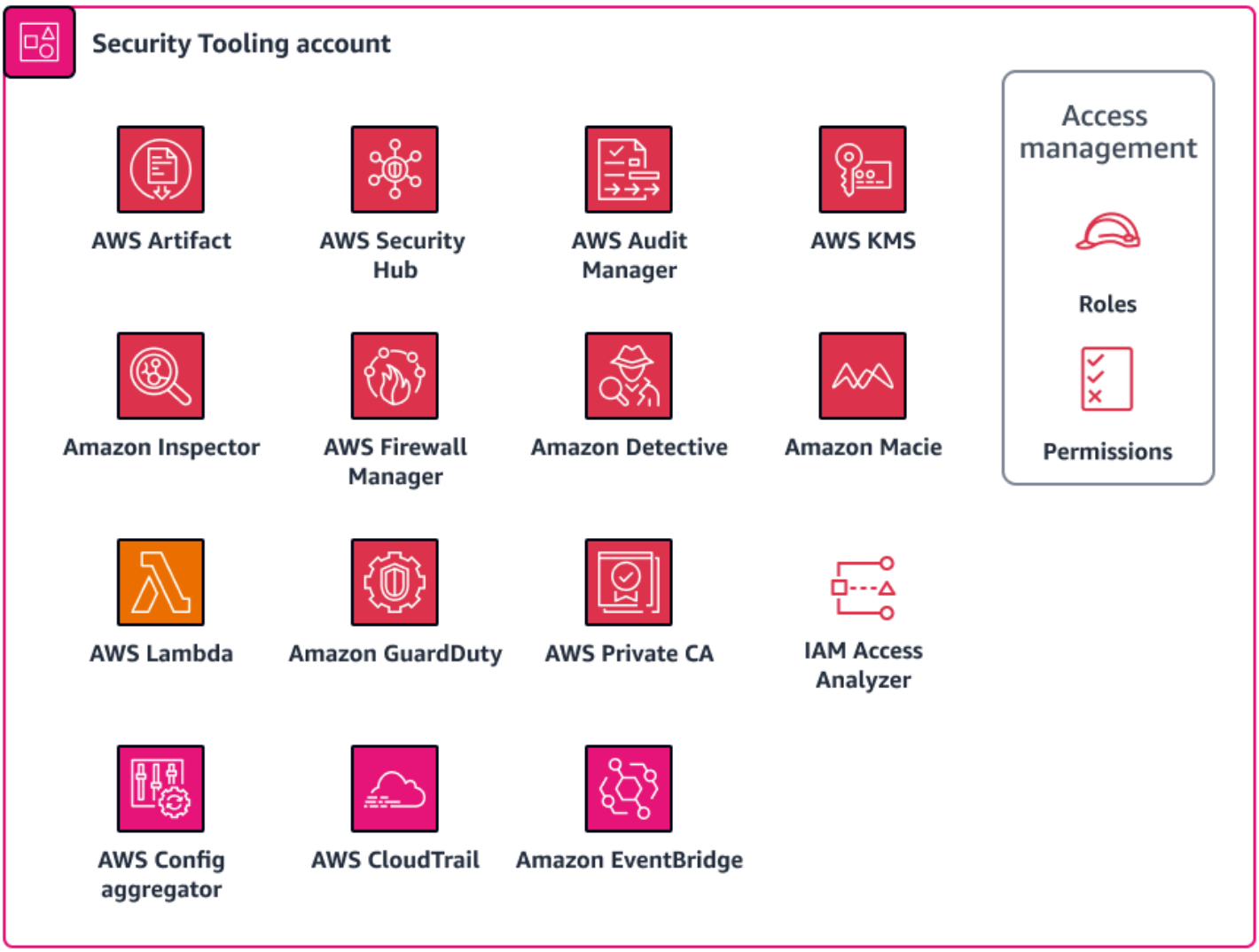
Quando utilizzi i tag come componente fondamentale della tua strategia di controllo della privacy, considera quanto segue:

- Considerate le implicazioni dell'inserimento di dati personali o altri tipi di dati sensibili all'interno delle chiavi o dei valori dei tag. Quando richiedi AWS assistenza tecnica, AWS potresti analizzare tag e altri identificatori di risorse per risolvere il problema. In questo caso, potresti voler rendere anonimi i valori dei tag e quindi reidentificarli utilizzando un sistema controllato dal cliente, come un sistema di gestione dei servizi IT (ITSM). AWS consiglia di non includere informazioni di identificazione personale nei tag.
- Tieni presente che alcuni valori dei tag devono essere resi immutabili (non modificabili) per evitare l'elusione dei controlli tecnici, come le condizioni ABAC che si basano sui tag.

Security OU — Account Security Tooling

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

L'account Security Tooling è dedicato alla gestione dei servizi fondamentali per la sicurezza e la privacy, al monitoraggio Account AWS e all'automazione degli avvisi e delle risposte in materia di sicurezza e privacy. Per ulteriori informazioni su questo account, consulta la AWS Security Reference Architecture (SRA).AWS Il diagramma seguente illustra i servizi AWS di sicurezza e privacy configurati nell'account Security Tooling.



Questa sezione fornisce informazioni più dettagliate su quanto segue in questo account:

- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- Sistema di analisi degli accessi IAM
- Amazon Macie

AWS CloudTrail

AWS CloudTrailti aiuta a controllare l'attività complessiva dell'API nel tuo Account AWS. Consentire CloudTrail a tutti Account AWS di archiviare, elaborare o trasmettere dati personali può aiutarti a

tenere traccia dell'uso e della divulgazione di questi dati. Regioni AWS La AWS Security Reference Architecture consiglia di abilitare un percorso organizzativo, ovvero un percorso singolo che registra tutti gli eventi per tutti gli account dell'organizzazione. Tuttavia, l'attivazione di questo percorso organizzativo aggrega i dati di log multiregionali in un unico bucket Amazon Simple Storage Service (Amazon S3) nell'account Log Archive. Per gli account che gestiscono dati personali, ciò può comportare alcune considerazioni di progettazione aggiuntive. I record di registro potrebbero contenere alcuni riferimenti a dati personali. Per soddisfare i requisiti di residenza e trasferimento dei dati, potrebbe essere necessario riconsiderare l'aggregazione dei dati di registro interregionali in un'unica regione in cui si trova il bucket S3. La tua organizzazione potrebbe valutare quali carichi di lavoro regionali includere o escludere dal percorso organizzativo. Per i carichi di lavoro che decidi di escludere dall'itinerario organizzativo, potresti prendere in considerazione la configurazione di un percorso specifico per regione che nasconda i dati personali. Per ulteriori informazioni sul mascheramento dei dati personali, consulta la Amazon Data Firehose sezione di questa guida. In definitiva, l'organizzazione potrebbe disporre di una combinazione di percorsi organizzativi e percorsi regionali aggregati nell'account Log Archive centralizzato.

Per ulteriori informazioni sulla configurazione di un percorso a regione singola, consulta le istruzioni per l'uso di AWS Command Line Interface (AWS CLI) o della console. Quando crei l'itinerario organizzativo, puoi utilizzare un'impostazione di attivazione in AWS Control Toweroppure puoi creare il percorso direttamente nella console. CloudTrail

Per ulteriori informazioni sull'approccio generale e su come gestire la centralizzazione dei log e i requisiti di trasferimento dei dati, consulta la Archiviazione centralizzata dei log sezione di questa guida. A prescindere dalla configurazione scelta, secondo lo SRA, potresti voler separare la gestione dei trail nell'account Security Tooling dall'archiviazione dei log nell'account Log Archive. AWS Questo design consente di creare politiche di accesso con privilegi minimi per coloro che devono gestire i log e per coloro che devono utilizzare i dati di registro.

AWS Config

AWS Configfornisce una visualizzazione dettagliata delle risorse presenti Account AWS e di come sono configurate. Ti aiuta a identificare in che modo le risorse si relazionano tra loro e in che modo le loro configurazioni sono cambiate nel tempo. Per ulteriori informazioni su come questo servizio viene utilizzato in un contesto di sicurezza, consulta la AWS Security Reference Architecture.

In AWS Config, è possibile distribuire pacchetti di conformità, che sono insiemi di AWS Config regole e azioni correttive. I Conformance Pack forniscono un framework generico progettato per consentire controlli di governance relativi a privacy, sicurezza, operatività e ottimizzazione dei costi utilizzando

regole gestite o personalizzate. AWS Config È possibile utilizzare questo strumento come parte di un set più ampio di strumenti di automazione per verificare se le configurazioni delle AWS risorse sono conformi ai requisiti del proprio framework di controllo.

Il pacchetto di conformità Operational Best Practices for NIST Privacy Framework v1.0 è allineato a una serie di controlli relativi alla privacy del NIST Privacy Framework. Ogni AWS Config regola si applica a un tipo di AWS risorsa specifico e si riferisce a uno o più controlli del NIST Privacy Framework. Puoi utilizzare questo pacchetto di conformità per monitorare la conformità continua relativa alla privacy tra le risorse dei tuoi account. Di seguito sono riportate alcune delle regole incluse in questo pacchetto di conformità:

- `no-unrestricted-route-to-igw`— Questa regola aiuta a prevenire l'esfiltrazione dei dati sul piano dati monitorando continuamente le tabelle di routing VPC per individuare percorsi predefiniti `0.0.0.0/0` o di `::/0` uscita verso un gateway Internet. Ciò consente di limitare i punti in cui può essere inviato il traffico diretto a Internet, soprattutto se esistono intervalli CIDR noti per essere dannosi.
- `encrypted-volumes`— Questa regola verifica se i volumi Amazon Elastic Block Store (Amazon EBS) collegati alle istanze di Amazon Elastic Compute Cloud (EC2Amazon) sono crittografati. Se la tua organizzazione ha requisiti di controllo specifici relativi all'uso delle chiavi AWS Key Management Service (AWS KMS) per la protezione dei dati personali, puoi specificare una chiave specifica IDs come parte della regola per verificare che i volumi siano crittografati con una chiave specifica. AWS KMS
- `restricted-common-ports`— Questa regola verifica se i gruppi EC2 di sicurezza Amazon consentono il traffico TCP senza restrizioni verso porte specifiche. I gruppi di sicurezza possono aiutarti a gestire l'accesso alla rete fornendo un filtraggio statico del traffico di rete in ingresso e in uscita verso le risorse. AWS Il blocco del traffico in ingresso dalle `0.0.0.0/0` porte comuni, come TCP 3389 e TCP 21, sulle risorse consente di limitare l'accesso remoto.

AWS Config può essere utilizzato per controlli di conformità proattivi e reattivi delle risorse. AWS Oltre a considerare le regole contenute nei pacchetti di conformità, è possibile incorporarle in modalità di valutazione sia investigativa che proattiva. Ciò consente di implementare i controlli sulla privacy nelle fasi iniziali del ciclo di vita di sviluppo del software, poiché gli sviluppatori di applicazioni possono iniziare a incorporare i controlli di predistribuzione. Ad esempio, possono includere nei AWS CloudFormation modelli degli hook che controllano la risorsa dichiarata nel modello rispetto a tutte le regole relative alla privacy che hanno la modalità proattiva AWS Config abilitata. Per ulteriori informazioni, consulta AWS Config Rules Now Support Proactive Compliance (post AWS del blog).

Amazon GuardDuty

AWS offre diversi servizi che possono essere utilizzati per archiviare o elaborare dati personali, come Amazon S3, Amazon Relational Database Service (Amazon RDS) o Amazon with Kubernetes. EC2 Amazon GuardDuty combina la visibilità intelligente con il monitoraggio continuo per rilevare indicatori che potrebbero essere correlati alla divulgazione involontaria di dati personali. Per ulteriori informazioni su come questo servizio viene utilizzato in un contesto di sicurezza, consulta la AWS Security Reference Architecture.

Con GuardDuty, puoi identificare attività potenzialmente dannose legate alla privacy durante tutto il ciclo di vita di un attacco. Ad esempio, GuardDuty può avvisarti in caso di connessioni a siti nella lista nera, traffico o volumi di traffico insoliti sulle porte di rete, esfiltrazioni DNS, avvii imprevisti di istanze e chiamate ISP insolite. EC2 È inoltre possibile configurare in modo GuardDuty da bloccare gli avvisi relativi agli indirizzi IP attendibili presenti nei propri elenchi di IP attendibili e segnalare gli indirizzi IP dannosi noti presenti nei propri elenchi di minacce.

Come consigliato nell' AWS SRA, è possibile attivare l'opzione GuardDuty per tutti i membri Account AWS dell'organizzazione e configurare l'account Security Tooling come amministratore delegato. GuardDuty GuardDutyaggrega i risultati provenienti da tutta l'organizzazione in un unico account. Per ulteriori informazioni, consulta Gestire GuardDuty gli account con AWS Organizations. Puoi anche prendere in considerazione l'identificazione di tutte le parti interessate legate alla privacy nel processo di risposta agli incidenti, dal rilevamento e dall'analisi al contenimento e all'eliminazione, e coinvolgerle in eventuali incidenti che potrebbero comportare l'esfiltrazione di dati.

Sistema di analisi degli accessi IAM

Molti clienti desiderano la garanzia continua che i dati personali vengano condivisi in modo appropriato con processori terzi preapprovati e previsti e nessun altro ente. Un perimetro di dati è un insieme di barriere preventive progettate per consentire solo alle identità attendibili delle reti previste di accedere a risorse affidabili nell'ambiente in uso. AWS Quando si definiscono i controlli per la divulgazione involontaria e intenzionale dei dati personali, è possibile definire identità affidabili, risorse affidabili e reti previste.

Con AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), le organizzazioni possono definire una Account AWS zona di attendibilità e configurare gli avvisi per le violazioni di tale zona di fiducia. IAM Access Analyzer analizza le policy IAM per aiutare a identificare e risolvere l'accesso pubblico o tra account non intenzionali a risorse potenzialmente sensibili. IAM Access Analyzer utilizza la logica matematica e l'inferenza per generare risultati completi per le risorse a cui è possibile accedere dall'esterno di un. Account AWS Infine, per rispondere e correggere

le policy IAM eccessivamente permissive, puoi utilizzare IAM Access Analyzer per convalidare le policy esistenti rispetto alle best practice IAM e fornire suggerimenti. IAM Access Analyzer può generare una policy IAM con privilegi minimi basata sull'attività di accesso precedente di un responsabile IAM. Analizza CloudTrail i log e genera una policy che concede solo le autorizzazioni necessarie per continuare a eseguire tali attività.

Per ulteriori informazioni su come IAM Access Analyzer viene utilizzato in un contesto di sicurezza, consulta la Security Reference Architecture.AWS

Amazon Macie

Amazon Macie è un servizio che utilizza l'apprendimento automatico e il pattern matching per scoprire dati sensibili, fornisce visibilità sui rischi per la sicurezza dei dati e aiuta ad automatizzare le protezioni contro tali rischi. Macie genera risultati quando rileva potenziali violazioni delle policy o problemi con la sicurezza o la privacy dei bucket Amazon S3. Macie è un altro strumento che le organizzazioni possono utilizzare per implementare l'automazione al fine di supportare gli sforzi di conformità. Per ulteriori informazioni su come questo servizio viene utilizzato in un contesto di sicurezza, consulta la AWS Security Reference Architecture.

Macie è in grado di rilevare un elenco ampio e crescente di tipi di dati sensibili, tra cui informazioni di identificazione personale (PII), come nomi, indirizzi e altri attributi identificabili. Puoi persino creare identificatori di dati personalizzati per definire criteri di rilevamento che riflettano la definizione di dati personali della tua organizzazione.

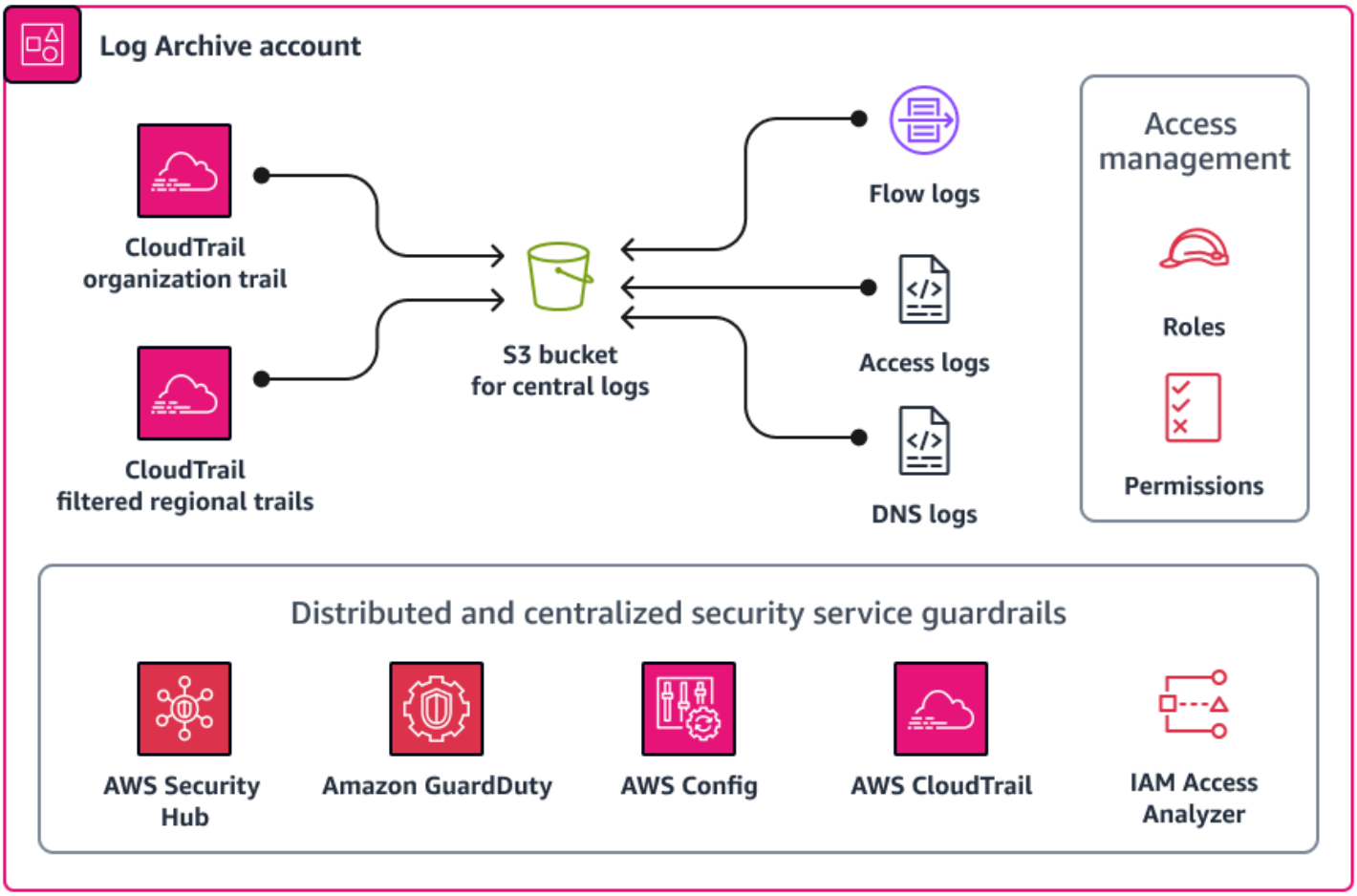
Man mano che la tua organizzazione definisce i controlli preventivi per i bucket Amazon S3 che contengono dati personali, puoi utilizzare Macie come meccanismo di convalida per fornire una rassicurazione continua su dove risiedono i tuoi dati personali e su come sono protetti. Per iniziare, abilita Macie e configura il rilevamento automatico dei dati sensibili. Macie analizza continuamente gli oggetti in tutti i bucket S3, tra account e. Regioni AWS Macie genera e mantiene una mappa termica interattiva che mostra dove risiedono i dati personali. La funzione di rilevamento automatico dei dati sensibili è progettata per ridurre i costi e ridurre al minimo la necessità di configurare manualmente i processi di rilevamento. Puoi sfruttare la funzionalità di rilevamento automatico dei dati sensibili e utilizzare Macie per rilevare automaticamente nuovi bucket o nuovi dati nei bucket esistenti e quindi convalidare i dati rispetto ai tag di classificazione dei dati assegnati. Configura questa architettura per notificare tempestivamente ai team di sviluppo e privacy appropriati i bucket erroneamente classificati o non classificati.

Puoi abilitare Macie per ogni account della tua organizzazione utilizzando. AWS Organizations Per ulteriori informazioni, consulta Integrazione e configurazione di un'organizzazione in Amazon Macie.

Security OU: account Log Archive

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

L'account Log Archive consente di centralizzare i tipi di registro dell'infrastruttura, dei servizi e delle applicazioni. Per ulteriori informazioni su questo account, consulta la AWS Security Reference Architecture (AWS SRA). Con un account dedicato per i registri, puoi applicare avvisi coerenti a tutti i tipi di registro e confermare che i soccorritori possano accedere a un insieme di questi registri da un'unica posizione. È inoltre possibile configurare i controlli di sicurezza e le politiche di conservazione dei dati da un'unica posizione, il che può semplificare il sovraccarico operativo relativo alla privacy. Il diagramma seguente illustra i servizi AWS di sicurezza e privacy configurati nell'account Log Archive.



Archiviazione centralizzata dei log

I file di registro (come AWS CloudTrail i registri) potrebbero contenere informazioni che potrebbero essere considerate dati personali. Alcune organizzazioni scelgono di utilizzare un percorso organizzativo per aggregare CloudTrail i log tra account Regioni AWS e account in un'unica posizione centrale, a fini di visibilità. Per ulteriori informazioni sul tagging, consulta AWS CloudTrailin questa guida. Quando si implementa la centralizzazione dei CloudTrail log, i log vengono generalmente archiviati in un bucket Amazon Simple Storage Service (Amazon S3) in un'unica regione.

A seconda della definizione di dati personali della tua organizzazione e delle normative regionali sulla privacy applicabili, potresti dover prendere in considerazione i trasferimenti di dati transfrontalieri. Se la tua organizzazione deve soddisfare i requisiti di trasferimento dei dati previsti dalle normative regionali sulla privacy, le seguenti opzioni possono aiutarti a supportare:

1. Se la tua organizzazione fornisce servizi Cloud AWS a interessati in più paesi, potresti scegliere di aggregare tutti i log nel paese che presenta i requisiti di residenza dei dati più rigorosi. Ad esempio, se operi in Germania e questo paese ha i requisiti più rigorosi, puoi aggregare i dati in un bucket S3 in modo che i dati raccolti in Germania non lascino i confini `eu-central-1` Regione AWS della Germania. Per questa opzione, puoi configurare un unico percorso organizzativo in CloudTrail cui i log di tutti gli account vengano aggregati nella regione di destinazione. Regioni AWS
2. Oscura i dati personali che devono rimanere archiviati Regione AWS prima che vengano copiati e aggregati in un'altra regione. Ad esempio, è possibile mascherare i dati personali nella regione ospitante dell'applicazione prima di trasferire i registri in un'altra regione. Per ulteriori informazioni sul mascheramento dei dati personali, consulta la Amazon Data Firehose sezione di questa guida.

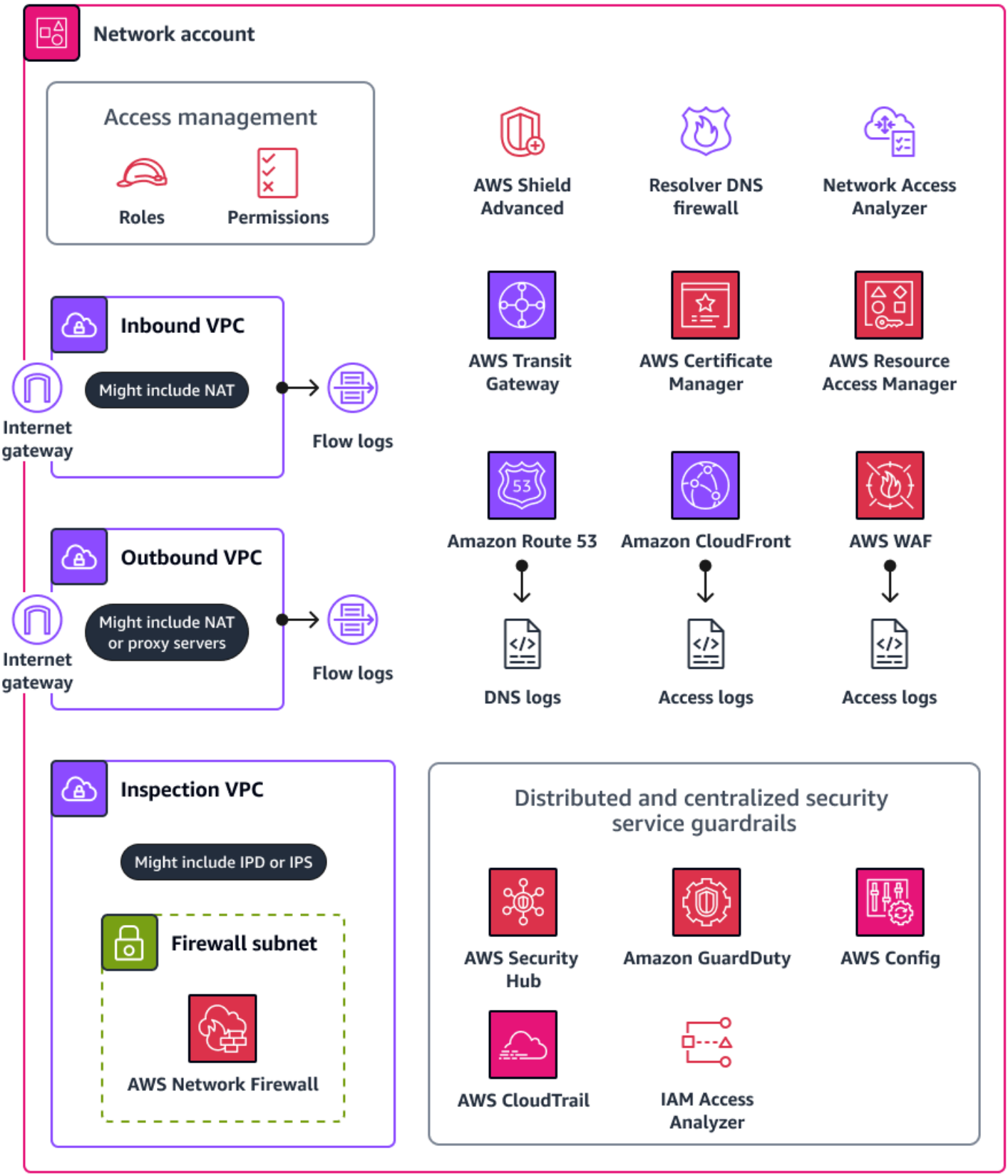
Rivolgiti al tuo consulente legale per determinare quali dati personali rientrano nell'ambito di applicazione e quali AWS Region-to-Region trasferimenti sono consentiti.

UO dell'infrastruttura - Account di rete

> Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Nell'account Network, gestisci la rete tra i tuoi cloud privati virtuali (VPCs) e Internet in generale. In questo account, puoi implementare ampi meccanismi di controllo della divulgazione utilizzando

AWS WAF, use AWS Resource Access Manager (AWS RAM) per condividere sottoreti AWS Transit Gateway e allegati VPC e utilizzare CloudFront Amazon per supportare l'utilizzo mirato del servizio. Per ulteriori informazioni su questo account, consulta la AWS Security Reference Architecture (SRA).AWS Il diagramma seguente illustra i servizi AWS di sicurezza e privacy configurati nell'account di rete.


Network account
Access management
Roles
Permissions
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
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

Questa sezione fornisce informazioni più dettagliate sui seguenti elementi Servizi AWS utilizzati in questo account:

- Amazon CloudFront
- AWS Resource Access Manager
- AWS Transit Gateway
- AWS WAF

Amazon CloudFront

Amazon CloudFront supporta restrizioni geografiche per le applicazioni frontend e l'hosting di file. CloudFrontè in grado di distribuire contenuti attraverso una rete mondiale di data center denominati edge location. Quando un utente richiede il contenuto che utilizzi CloudFront, la richiesta viene indirizzata all'edge location che offre la latenza più bassa. Per ulteriori informazioni su come questo servizio viene utilizzato in un contesto di sicurezza, consulta la AWS Security Reference Architecture.

Puoi utilizzare restrizioni CloudFront geografiche per impedire agli utenti di aree geografiche specifiche di accedere ai contenuti che stai distribuendo tramite una CloudFront distribuzione. Per ulteriori informazioni e opzioni di configurazione per le restrizioni geografiche, consulta Limitazione della distribuzione geografica dei contenuti nella CloudFront documentazione.

Puoi anche configurare la generazione CloudFront di registri di accesso che contengono informazioni dettagliate su ogni richiesta utente ricevuta. CloudFront Per ulteriori informazioni, consulta Configurazione e utilizzo dei log standard (log di accesso) nella documentazione. CloudFront Infine, se CloudFront è configurato per memorizzare nella cache i contenuti in una serie di edge location, è possibile considerare dove avviene la memorizzazione nella cache. Per alcune organizzazioni, la memorizzazione nella cache interregionale potrebbe essere soggetta a requisiti di trasferimento transfrontaliero dei dati.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) ti aiuta a condividere in modo sicuro le tue risorse Account AWS per ridurre il sovraccarico operativo e fornire visibilità e verificabilità. Con AWS RAM, le organizzazioni possono limitare le AWS risorse che possono essere condivise con altri Account AWS membri della propria organizzazione o con account di terze parti. Per ulteriori informazioni, consulta AWS Risorse condivisibili. Nell'account di rete, puoi utilizzarlo AWS RAM per condividere sottoreti VPC e connessioni gateway di transito. Se la utilizzi AWS RAM per condividere una connessione sul

piano dati con un'altra Account AWS, valuta la possibilità di stabilire dei processi per verificare che le connessioni siano preapprovate. Regioni AWS

Oltre alla condivisione VPCs e alle connessioni gateway di transito, AWS RAM possono essere utilizzate per condividere risorse che non supportano le policy basate sulle risorse IAM. Per un carico di lavoro ospitato nell'unità organizzativa per i dati personali, puoi utilizzarlo AWS RAM per accedere ai dati personali che si trovano in un'unità separata. Account AWS Per ulteriori informazioni, consulta AWS Resource Access Manager la sezione Account dell'applicazione Personal Data OU — PD.

AWS Transit Gateway

Se desideri distribuire AWS risorse che raccolgono, archiviano o trattano dati personali in Regioni AWS linea con i requisiti di residenza dei dati della tua organizzazione e disponi delle garanzie tecniche appropriate, prendi in considerazione l'implementazione di barriere per impedire flussi di dati transfrontalieri non approvati sui piani di controllo e dati. Sul piano di controllo, puoi limitare l'utilizzo della regione e, di conseguenza, i flussi di dati tra regioni utilizzando IAM e le politiche di controllo dei servizi.

Esistono diverse opzioni per controllare i flussi di dati tra regioni sul piano dati. Ad esempio, puoi utilizzare tabelle di routing, peering VPC e allegati. AWS Transit Gateway AWS Transit Gatewayè un hub centrale che collega cloud privati virtuali (VPCs) e reti locali. Come parte di una landing zone AWS più ampia, puoi prendere in considerazione i vari modi in cui i dati possono transitare Regioni AWS, tra cui i gateway Internet, il peering diretto e il VPC-to-VPC peering interregionale. AWS Transit Gateway Ad esempio, puoi fare quanto segue in: AWS Transit Gateway

- Verifica che le connessioni est-ovest e nord-sud tra il tuo ambiente VPCs e quello locale siano in linea con i tuoi requisiti di privacy.
- Configura le impostazioni del VPC in base ai tuoi requisiti di privacy.
- Utilizza una policy di controllo dei servizi AWS Organizations e policy IAM per prevenire modifiche alle tue configurazioni AWS Transit Gateway e a quelle di Amazon Virtual Private Cloud (Amazon VPC). Per un esempio di politica di controllo del servizio, consulta Limita le modifiche alle configurazioni VPC questa guida.

AWS WAF

Per evitare la divulgazione involontaria di dati personali, puoi implementare un defense-in-depth approccio per le tue applicazioni web. È possibile integrare la convalida degli input e la limitazione

della velocità nella propria applicazione, ma AWS WAF può fungere da ulteriore linea di difesa. AWS WAFè un firewall per applicazioni Web che consente di monitorare le richieste HTTP e HTTPS inoltrate alle risorse protette delle applicazioni Web. Per ulteriori informazioni su come questo servizio viene utilizzato in un contesto di sicurezza, consulta la AWS Security Reference Architecture.

Con AWS WAF, puoi definire e implementare regole che controllano criteri specifici. Le seguenti attività potrebbero essere associate alla divulgazione involontaria di dati personali:

- Traffico proveniente da indirizzi IP o località geografiche sconosciuti o dannosi
- I 10 principali attacchi dell'Open Worldwide Application Security Project (OWASP), inclusi gli attacchi legati all'esfiltrazione come l'iniezione SQL
- Elevate percentuali di richieste
- Traffico generale dei bot
- Scraper di contenuti

È possibile distribuire gruppi di AWS WAF regole gestiti da. AWS Alcuni gruppi di regole gestiti per AWS WAF possono essere utilizzati per rilevare minacce alla privacy e ai dati personali, ad esempio:

- Database SQL: questo gruppo di regole contiene regole progettate per bloccare i modelli di richiesta associati allo sfruttamento dei database SQL, come gli attacchi SQL injection. Considerate questo gruppo di regole se la vostra applicazione si interfaccia con un database SQL.
- Input noti non validi: questo gruppo di regole contiene regole progettate per bloccare modelli di richiesta noti per non essere validi e associati allo sfruttamento o all'individuazione di vulnerabilità.
- Bot Control: questo gruppo di regole contiene regole progettate per gestire le richieste dei bot, che possono consumare risorse in eccesso, alterare le metriche aziendali, causare tempi di inattività ed eseguire attività dannose.
- Prevenzione dell'acquisizione di account (ATP): questo gruppo di regole contiene regole progettate per prevenire tentativi malevoli di acquisizione di account. Questo gruppo di regole controlla i tentativi di accesso inviati all'endpoint di accesso dell'applicazione.

Dati personali OU — Account dell'applicazione PD

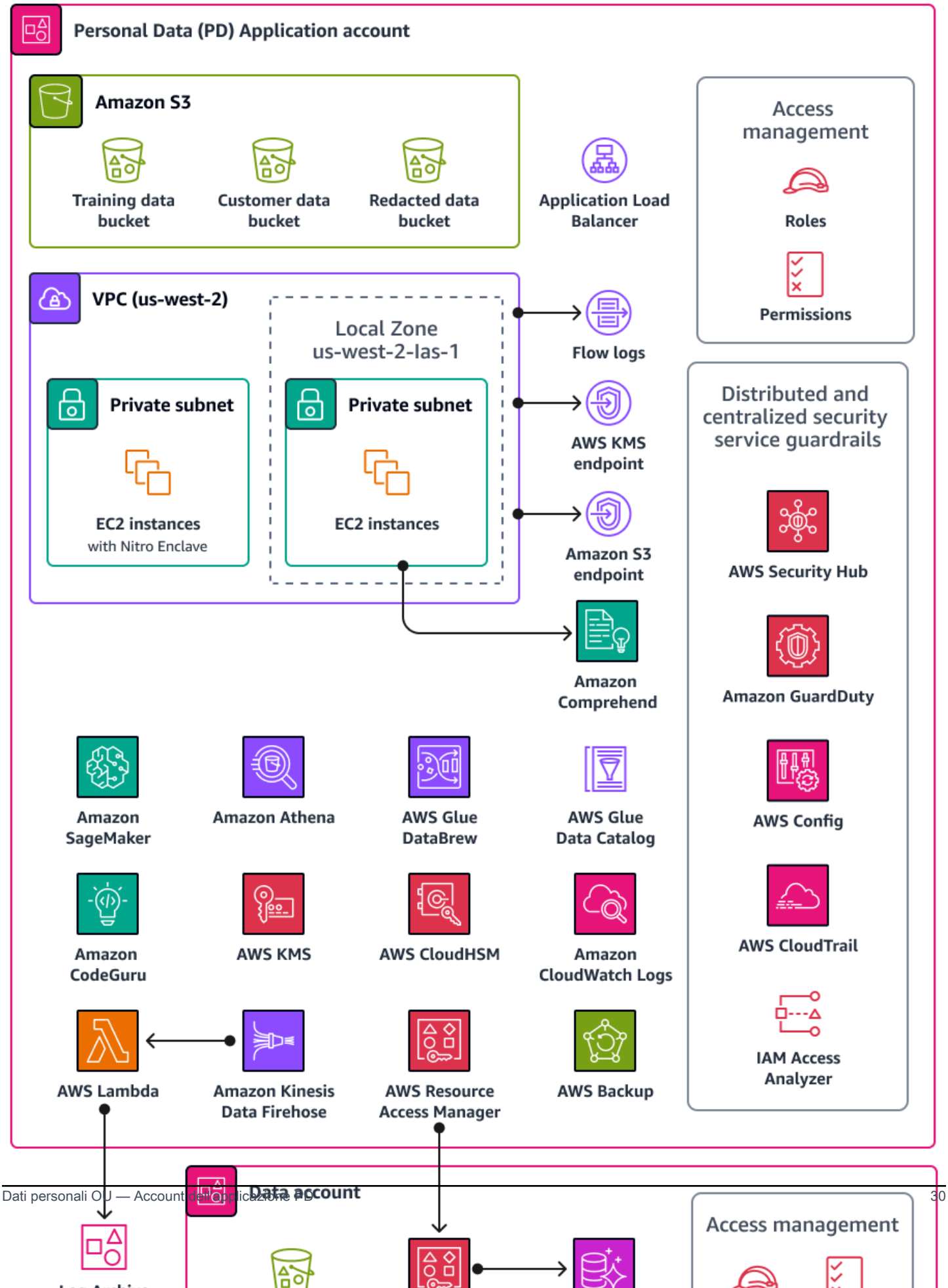
Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

L'account dell'applicazione per i dati personali (PD) è il luogo in cui la tua organizzazione ospita servizi che raccolgono ed elaborano dati personali. In particolare, potresti archiviare quelli che definisci come dati personali in questo account. Il AWS PRA illustra una serie di esempi di configurazioni di privacy attraverso un'architettura web serverless a più livelli. Quando si tratta di gestire carichi di lavoro in una AWS landing zone, le configurazioni di privacy non dovrebbero essere considerate one-size-fits-all soluzioni. Ad esempio, l'obiettivo potrebbe essere quello di comprendere i concetti di base, come possono migliorare la privacy e come l'organizzazione può applicare soluzioni a casi d'uso e architetture particolari.

Account AWS Nell'organizzazione che raccoglie, archivia o elabora dati personali, è possibile utilizzare AWS Organizations e AWS Control Tower implementare barriere di base e ripetibili. La creazione di un'unità organizzativa (OU) dedicata per questi account è fondamentale. Ad esempio, potresti voler applicare i limiti di residenza dei dati solo a un sottoinsieme di account in cui la residenza dei dati è una considerazione di progettazione fondamentale. Per molte organizzazioni, questi sono gli account che archiviano ed elaborano i dati personali.

La tua organizzazione potrebbe supportare un account Data dedicato, che è il luogo in cui archivi la fonte autorevole dei tuoi set di dati personali. Una fonte di dati autorevole è un luogo in cui è archiviata la versione principale dei dati, che potrebbe essere considerata la versione più affidabile e accurata dei dati. Ad esempio, puoi copiare i dati dalla fonte di dati autorevole in altre posizioni, come i bucket Amazon Simple Storage Service (Amazon S3) nell'account PD Application, utilizzati per archiviare dati di formazione, un sottoinsieme di dati dei clienti e dati oscurati. Adottando questo approccio multi-account per separare i set di dati personali completi e definitivi nell'account Data dai carichi di lavoro dei consumatori a valle nell'account PD Application, puoi ridurre l'ambito di impatto in caso di accesso non autorizzato ai tuoi account.

Il diagramma seguente illustra i servizi di AWS sicurezza e privacy configurati negli account PD Application and Data.


Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application Load Balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local Zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Amazon Comprehend
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon SageMaker
Amazon Athena
AWS Glue DataBrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Data account
Log Archive
Access management

Questa sezione fornisce informazioni più dettagliate sui seguenti elementi Servizi AWS utilizzati in questi account:

- Amazon Athena
- CloudWatch Registri Amazon
- CodeGuru Revisore Amazon
- Amazon Comprehend
- Amazon Data Firehose
- AWS Glue
- AWS Key Management Service
- AWS Local Zones
- AWS Enclavi Nitro
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker AI
- AWS funzionalità che aiutano a gestire il ciclo di vita dei dati
- Servizi e funzionalità AWS che aiutano a segmentare i dati

Amazon Athena

Puoi anche prendere in considerazione i controlli di limitazione delle interrogazioni sui dati per raggiungere i tuoi obiettivi di privacy. Amazon Athena è un servizio di query interattivo che ti aiuta ad analizzare i dati direttamente in Amazon S3 utilizzando SQL standard. Non è necessario caricare i dati in Athena; funziona direttamente con i dati archiviati nei bucket S3.

Un caso d'uso comune per Athena è fornire ai team di analisi dei dati set di dati personalizzati e sanificati. Se i set di dati contengono dati personali, puoi disinfettare il set di dati mascherando intere colonne di dati personali che forniscono poco valore ai team di analisi dei dati. Per ulteriori informazioni, consulta Rendere anonimi e gestire i dati nel tuo data lake con Amazon Athena AWS Lake Formation e AWS (post sul blog).

Se il tuo approccio alla trasformazione dei dati richiede una flessibilità aggiuntiva oltre alle funzioni supportate in Athena, puoi definire funzioni personalizzate, chiamate funzioni definite dall'utente (UDF). È possibile richiamarle UDFs in una query SQL inviata ad Athena ed eseguirle. AWS

LambdaÈ possibile utilizzare UDFs le `FILTER SQL` query `SELECT` e richiamarne più di una UDFs nella stessa query. Per motivi di privacy, è possibile creare UDFs sistemi che eseguano tipi specifici di mascheramento dei dati, ad esempio mostrando solo gli ultimi quattro caratteri di ogni valore in una colonna.

CloudWatch Registri Amazon

Amazon CloudWatch Logs ti aiuta a centralizzare i log di tutti i tuoi sistemi e applicazioni, Servizi AWS così puoi monitorarli e archiviarli in modo sicuro. In CloudWatch Logs, puoi utilizzare una politica di protezione dei dati per gruppi di log nuovi o esistenti per ridurre al minimo il rischio di divulgazione di dati personali. Le politiche di protezione dei dati possono rilevare dati sensibili, come i dati personali, nei registri. La politica di protezione dei dati può mascherare tali dati quando gli utenti accedono ai registri tramite. AWS Management Console Quando gli utenti richiedono l'accesso diretto ai dati personali, in base alle specifiche generali dello scopo del carico di lavoro, è possibile assegnare `logs:Unmask` le autorizzazioni a tali utenti. Puoi anche creare una politica di protezione dei dati a livello di account e applicarla in modo coerente a tutti gli account della tua organizzazione. Questo configura il mascheramento per impostazione predefinita per tutti i gruppi di log attuali e futuri in CloudWatch Logs. Ti consigliamo inoltre di abilitare i report di controllo e di inviarli a un altro gruppo di log, a un bucket Amazon S3 o Amazon Data Firehose. Questi report contengono un registro dettagliato dei risultati sulla protezione dei dati in ogni gruppo di log.

CodeGuru Revisore Amazon

Sia per la privacy che per la sicurezza, è fondamentale per molte organizzazioni supportare la conformità continua durante le fasi di implementazione e post-implementazione. Il AWS PRA include controlli proattivi nelle pipeline di implementazione per le applicazioni che elaborano dati personali. Amazon CodeGuru Reviewer è in grado di rilevare potenziali difetti che potrebbero esporre i dati personali nel codice Java e Python. JavaScript Offre suggerimenti agli sviluppatori per migliorare il codice. CodeGuru Reviewer è in grado di identificare i difetti relativi a un'ampia gamma di procedure consigliate in materia di sicurezza, privacy e generali. Per ulteriori informazioni, consulta Amazon CodeGuru Detector Library. È progettato per funzionare con più provider di sorgenti AWS CodeCommit, tra cui Bitbucket e Amazon GitHub S3. Alcuni dei difetti relativi alla privacy che Reviewer è in grado di rilevare includono: CodeGuru

- iniezione SQL
- Cookie non protetti
- Autorizzazione mancante

- Ricrittografia lato client AWS KMS

Amazon Comprehend

Amazon Comprehend è un servizio di elaborazione del linguaggio naturale (NLP) che utilizza l'apprendimento automatico per scoprire informazioni e connessioni preziose nei documenti di testo in inglese. Amazon Comprehend è in grado di rilevare e redigere dati personali in documenti di testo strutturati, semistrutturati o non strutturati. Per ulteriori informazioni, consulta Informazioni di identificazione personale (PII) nella documentazione di Amazon Comprehend.

Puoi utilizzare l'API AWS SDKs e Amazon Comprehend per integrare Amazon Comprehend con molte applicazioni. Un esempio è l'utilizzo di Amazon Comprehend per rilevare e redigere dati personali con Amazon S3 Object Lambda. Le organizzazioni possono utilizzare S3 Object Lambda per aggiungere codice personalizzato alle richieste Amazon S3 GET per modificare ed elaborare i dati non appena vengono restituiti a un'applicazione. S3 Object Lambda può filtrare le righe, ridimensionare dinamicamente le immagini, oscurare i dati personali e altro ancora. Basato sulle AWS Lambda funzioni, il codice viene eseguito su un'infrastruttura completamente gestita da AWS, il che elimina la necessità di creare e archiviare copie derivate dei dati o di eseguire proxy. Non è necessario modificare le applicazioni per trasformare gli oggetti con S3 Object Lambda. Puoi utilizzare la funzione `ComprehendPiiRedactionS3Object` Lambda per AWS Serverless Application Repository oscurare i dati personali. Questa funzione utilizza Amazon Comprehend per rilevare le entità di dati personali e oscura tali entità sostituendole con asterischi. Per ulteriori informazioni, consulta Rilevamento e redazione dei dati PII con S3 Object Lambda e Amazon Comprehend nella documentazione di Amazon S3.

Poiché Amazon Comprehend offre molte opzioni per l'integrazione delle applicazioni tramite AWS SDKs, puoi utilizzare Amazon Comprehend per identificare i dati personali in molti luoghi diversi in cui li raccogli, archivia ed elabora. Puoi utilizzare le funzionalità di Amazon Comprehend ML per rilevare e redigere i dati personali nei log delle applicazioni (post del AWS blog), nelle e-mail dei clienti, nei ticket di assistenza e altro ancora. Il diagramma di architettura per l'account PD Application mostra come eseguire questa funzione per i log delle applicazioni su Amazon. EC2 Amazon Comprehend offre due modalità di redazione:

- `REPLACE_WITH_PII_ENTITY_TYPE`sostituisce ogni entità PII con i relativi tipi. Ad esempio, Jane Doe verrebbe sostituita da NAME.
- `MASK`sostituisce i caratteri delle entità PII con un carattere a tua scelta (! , #, $,%, &, o @). Ad esempio, Jane Doe potrebbe essere sostituita con **** ***.

Amazon Data Firehose

Amazon Data Firehose può essere utilizzato per acquisire, trasformare e caricare dati di streaming in servizi downstream, come Amazon Managed Service per Apache Flink o Amazon S3. Firehose viene spesso utilizzato per trasportare grandi quantità di dati in streaming, come i log delle applicazioni, senza dover creare pipeline di elaborazione da zero.

È possibile utilizzare le funzioni Lambda per eseguire elaborazioni personalizzate o integrate prima che i dati vengano inviati a valle. Per quanto riguarda la privacy, questa funzionalità supporta la riduzione al minimo dei dati e i requisiti di trasferimento transfrontaliero dei dati. Ad esempio, è possibile utilizzare Lambda e Firehose per trasformare i dati di registro multiregione prima che siano centralizzati nell'account Log Archive. Per ulteriori informazioni, vedete Biogen: soluzione di registrazione centralizzata per più account (video). YouTube Nell'account PD Application, puoi configurare Amazon CloudWatch e inviare i log AWS CloudTrail a un flusso di distribuzione Firehose. Una funzione Lambda trasforma i log e li invia a un bucket S3 centrale nell'account Log Archive. È possibile configurare la funzione Lambda per mascherare campi specifici che contengono dati personali. Questo aiuta a prevenire il trasferimento di dati personali da una parte all'altra Regioni AWS. Utilizzando questo approccio, i dati personali vengono mascherati prima del trasferimento e della centralizzazione, anziché dopo. Per le applicazioni in giurisdizioni che non sono soggette ai requisiti di trasferimento transfrontaliero, in genere è più efficiente dal punto di vista operativo ed economico aggregare i log attraverso il percorso organizzativo. CloudTrail Per ulteriori informazioni, vedere AWS CloudTrail la sezione Security OU — Security Tooling account di questa guida.

AWS Glue

La manutenzione dei set di dati che contengono dati personali è un componente chiave di Privacy by Design. I dati di un'organizzazione possono esistere in forme strutturate, semistrutturate o non strutturate. I set di dati personali privi di struttura possono rendere difficile l'esecuzione di una serie di operazioni di miglioramento della privacy, tra cui la riduzione al minimo dei dati, il rintracciamento dei dati attribuiti a un singolo interessato come parte di una richiesta dell'interessato, la garanzia di una qualità costante dei dati e la segmentazione complessiva dei set di dati. AWS Glueè un servizio di estrazione, trasformazione e caricamento (ETL) completamente gestito. Può aiutarti a classificare, pulire, arricchire e spostare i dati tra archivi di dati e flussi di dati. AWS Glue le funzionalità sono progettate per aiutarti a scoprire, preparare, strutturare e combinare set di dati per l'analisi, l'apprendimento automatico e lo sviluppo di applicazioni. È possibile utilizzarle AWS Glue per creare una struttura prevedibile e comune in aggiunta ai set di dati esistenti. AWS Glue Data Catalog AWS Glue DataBrew, e AWS Glue Data Quality sono AWS Glue funzionalità che possono aiutare a supportare i requisiti di privacy dell'organizzazione.

AWS Glue Data Catalog

AWS Glue Data Catalogti aiuta a stabilire set di dati gestibili. Il Data Catalog contiene riferimenti ai dati utilizzati come fonti e destinazioni per i processi di estrazione, trasformazione e caricamento (ETL). AWS Glue Le informazioni nel Data Catalog vengono archiviate come tabelle di metadati e ogni tabella specifica un singolo archivio dati. Esegui un AWS Glue crawler per fare l'inventario dei dati in una varietà di tipi di data store. Si aggiungono classificatori incorporati e personalizzati al crawler e questi classificatori deducono il formato e lo schema dei dati personali. Il crawler scrive quindi i metadati nel Data Catalog. Una tabella di metadati centralizzata può semplificare la risposta alle richieste degli interessati (ad esempio il diritto alla cancellazione) perché aggiunge struttura e prevedibilità tra le diverse fonti di dati personali presenti nell'ambiente. AWS Per un esempio completo di come utilizzare Data Catalog per rispondere automaticamente a queste richieste, consulta Gestione delle richieste di cancellazione dei dati nel tuo data lake con Amazon S3 Find and Forget AWS (post del blog). Infine, se la tua organizzazione è abituata AWS Lake Formationad amministrare e fornire un accesso granulare a database, tabelle, righe e celle, Data Catalog è un componente chiave. Data Catalog offre la condivisione dei dati tra account e ti aiuta a utilizzare il controllo degli accessi basato su tag per gestire il tuo data lake su larga scala (post del blog).AWS

AWS Glue DataBrew

AWS Glue DataBrewti aiuta a pulire e normalizzare i dati e può eseguire trasformazioni sui dati, come rimuovere o mascherare le informazioni di identificazione personale e crittografare i campi di dati sensibili nelle pipeline di dati. Puoi anche mappare visivamente la provenienza dei tuoi dati per comprendere le varie fonti di dati e le fasi di trasformazione che i dati hanno subito. Questa funzionalità diventa sempre più importante man mano che l'organizzazione lavora per comprendere e tracciare meglio la provenienza dei dati personali. DataBrew ti aiuta a mascherare i dati personali durante la preparazione dei dati. È possibile rilevare i dati personali nell'ambito di un processo di profilazione dei dati e raccogliere statistiche, come il numero di colonne che potrebbero contenere dati personali e potenziali categorie. È quindi possibile utilizzare le tecniche integrate di trasformazione dei dati reversibili o irreversibili, tra cui la sostituzione, l'hashing, la crittografia e la decrittografia, il tutto senza scrivere alcun codice. È quindi possibile utilizzare i set di dati puliti e mascherati a valle per attività di analisi, reportistica e apprendimento automatico. Alcune delle tecniche di mascheramento dei dati disponibili includono: DataBrew

- Hashing: applica le funzioni di hash ai valori delle colonne.
- Sostituzione: sostituisci i dati personali con altri valori dall'aspetto autentico.
- Annullamento o eliminazione: sostituisci un campo particolare con un valore nullo o elimina la colonna.

- Mascheratura: usa il rimescolamento dei caratteri o maschera determinate parti delle colonne.

Le seguenti sono le tecniche di crittografia disponibili:

- Crittografia deterministica: applica algoritmi di crittografia deterministica ai valori delle colonne. La crittografia deterministica produce sempre lo stesso testo cifrato per un valore.
- Crittografia probabilistica: applica algoritmi di crittografia probabilistica ai valori delle colonne. La crittografia probabilistica produce un testo cifrato diverso ogni volta che viene applicata.

Per un elenco completo delle ricette di trasformazione dei dati personali fornite in DataBrew, consulta Procedure introduttive relative alle informazioni di identificazione personale (PII).

AWS Glue Qualità dei dati

AWS Glue Data Quality ti aiuta ad automatizzare e rendere operativa la distribuzione di dati di alta qualità attraverso le pipeline di dati, in modo proattivo, prima che vengano consegnati ai tuoi consumatori di dati. AWS Glue Data Quality fornisce un'analisi statistica dei problemi di qualità dei dati nelle tue pipeline di dati, può attivare avvisi in Amazon EventBridge e può formulare raccomandazioni sulle regole di qualità per la correzione. AWS Glue Data Quality supporta anche la creazione di regole con un linguaggio specifico del dominio in modo da poter creare regole di qualità dei dati personalizzate.

AWS Key Management Service

AWS Key Management Service (AWS KMS) consente di creare e controllare chiavi crittografiche per proteggere i dati. AWS KMS utilizza moduli di sicurezza hardware per proteggere e convalidare AWS KMS keys nell'ambito del programma di convalida dei moduli crittografici FIPS 140-2. Per ulteriori informazioni su come questo servizio viene utilizzato in un contesto di sicurezza, vedere Security Reference Architecture.AWS

AWS KMS si integra con la maggior parte delle aziende Servizi AWS che offrono la crittografia e consente di utilizzare le chiavi KMS nelle applicazioni che elaborano e archiviano dati personali. Puoi utilizzarle AWS KMS per supportare una serie di requisiti di privacy e salvaguardare i dati personali, tra cui:

- Utilizzo di chiavi gestite dal cliente per un maggiore controllo su forza, rotazione, scadenza e altre opzioni.

- Utilizzo di chiavi dedicate gestite dal cliente per proteggere i dati personali e i segreti che consentono l'accesso ai dati personali.
- Definizione dei livelli di classificazione dei dati e designazione di almeno una chiave dedicata gestita dal cliente per livello. Ad esempio, potresti avere una chiave per crittografare i dati operativi e un'altra per crittografare i dati personali.
- Impedire l'accesso involontario tra account alle chiavi KMS.
- Archiviazione delle chiavi KMS all'interno della Account AWS stessa risorsa da crittografare.
- Implementazione della separazione dei compiti per l'amministrazione e l'utilizzo delle chiavi KMS. Per ulteriori informazioni, consulta Come usare KMS e IAM per abilitare controlli di sicurezza indipendenti per i dati crittografati in S3 (AWS post del blog).
- Imposizione della rotazione automatica delle chiavi attraverso barriere preventive e reattive.

Per impostazione predefinita, le chiavi KMS vengono archiviate e possono essere utilizzate solo nella regione in cui sono state create. Se la tua organizzazione ha requisiti specifici per la residenza e la sovranità dei dati, valuta se le chiavi KMS multiregionali sono appropriate per il tuo caso d'uso. Le chiavi multiregionali sono chiavi KMS per scopi speciali, diverse tra loro, che possono essere utilizzate in modo intercambiabile. Regioni AWS Il processo di creazione di una chiave multiregionale sposta il materiale chiave oltre Regione AWS i confini interni AWS KMS, quindi questa mancanza di isolamento regionale potrebbe non essere compatibile con gli obiettivi di conformità dell'organizzazione. Un modo per risolvere questo problema consiste nell'utilizzare un tipo diverso di chiave KMS, ad esempio una chiave gestita dal cliente specifica per regione.

AWS Local Zones

Se è necessario rispettare i requisiti di residenza dei dati, è possibile implementare risorse che archiviano ed elaborano i dati personali specificamente Regioni AWS per supportare tali requisiti. Puoi anche utilizzare AWS Local Zones, che ti aiuta a collocare risorse di elaborazione, storage, database e altre AWS risorse selezionate vicino a grandi centri abitati e industriali. Una zona locale è un'estensione di una zona Regione AWS che si trova in prossimità geografica di una grande area metropolitana. È possibile collocare tipi specifici di risorse all'interno di una zona locale, vicino alla regione a cui corrisponde la zona locale. Le Local Zones possono aiutarti a soddisfare i requisiti di residenza dei dati quando una regione non è disponibile all'interno della stessa giurisdizione legale. Quando utilizzi Local Zones, prendi in considerazione i controlli di residenza dei dati implementati all'interno della tua organizzazione. Ad esempio, potrebbe essere necessario un controllo per impedire il trasferimento di dati da una zona locale specifica a un'altra regione. Per ulteriori informazioni su come utilizzare per mantenere le barriere SCPs per il trasferimento transfrontaliero

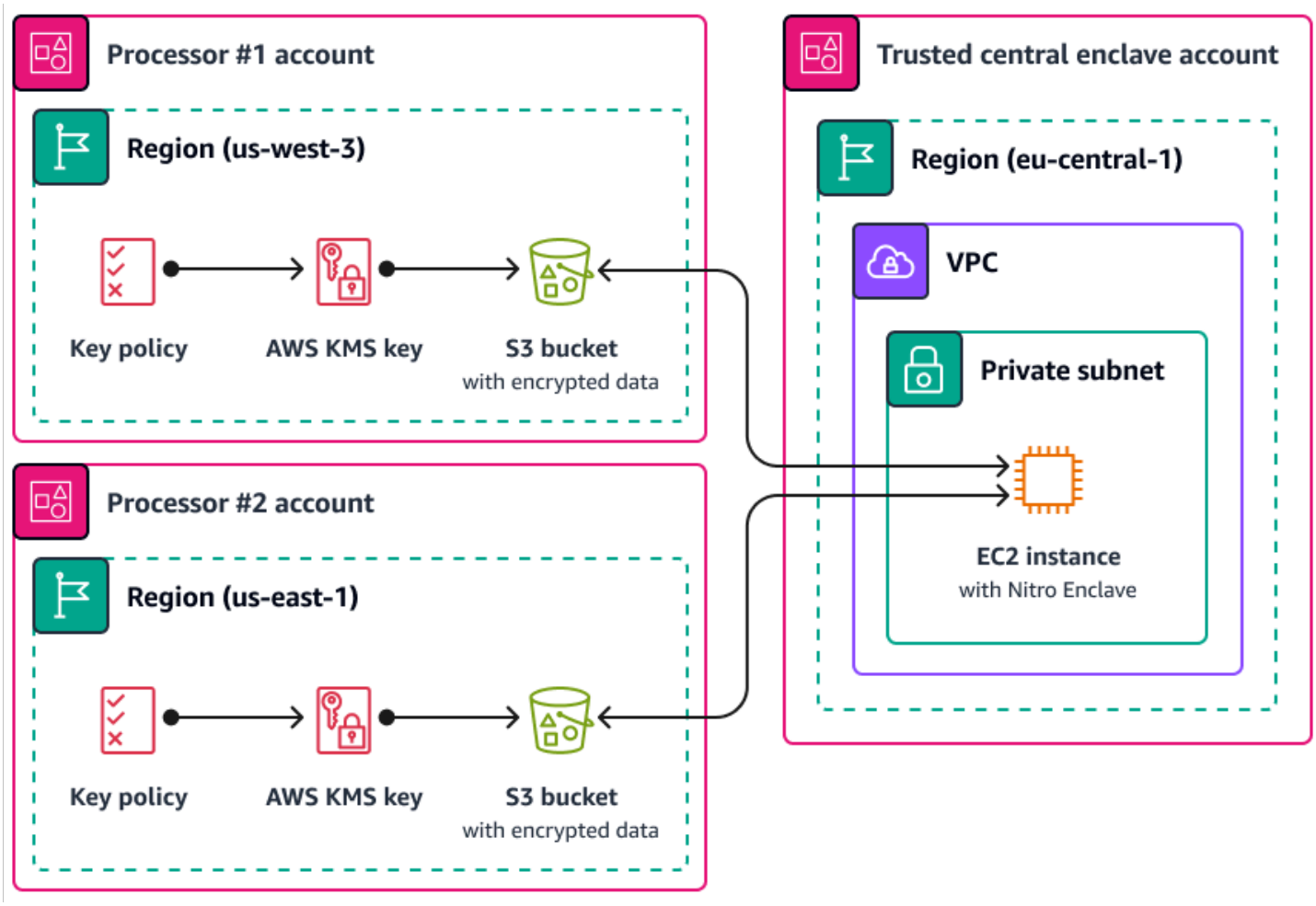
dei dati, consulta Best Practices for managing data residency in Local Zones AWS using landing zone control (AWS post sul blog).

AWS Enclavi Nitro

Considera la tua strategia di segmentazione dei dati dal punto di vista dell'elaborazione, ad esempio l'elaborazione dei dati personali con un servizio di elaborazione come Amazon Elastic Compute Cloud (Amazon). EC2 L'elaborazione riservata come parte di una strategia di architettura più ampia può aiutarti a isolare l'elaborazione dei dati personali in un'enclave di CPU isolata, protetta e affidabile. Le enclavi sono macchine virtuali separate, rinforzate e altamente vincolate. AWS Nitro Enclaves è una EC2 funzionalità di Amazon che può aiutarti a creare questi ambienti di elaborazione isolati. Per ulteriori informazioni, consulta The Security Design of the AWS Nitro System (white paper).AWS

Nitro Enclaves distribuisce un kernel separato dal kernel dell'istanza principale. Il kernel dell'istanza principale non ha accesso all'enclave. Gli utenti non possono utilizzare SSH o accedere in remoto ai dati e alle applicazioni nell'enclave. Le applicazioni che elaborano dati personali possono essere incorporate nell'enclave e configurate per utilizzare il Vsock dell'enclave, il socket che facilita la comunicazione tra l'enclave e l'istanza principale.

Un caso d'uso in cui Nitro Enclaves può essere utile è l'elaborazione congiunta tra due processori di dati separati e che potrebbero non fidarsi l'uno dell'altro. Regioni AWS L'immagine seguente mostra come utilizzare un'enclave per l'elaborazione centralizzata, una chiave KMS per crittografare i dati personali prima che vengano inviati all'enclave e una AWS KMS key politica che verifica che l'enclave che richiede la decrittografia abbia le misure uniche nel documento di attestazione. Per AWS KMS ulteriori informazioni e istruzioni, consulta Utilizzo dell'attestazione crittografica con. Per un esempio di policy chiave, consulta questa Richiedi l'attestazione per utilizzare una chiave AWS KMS guida.



Con questa implementazione, solo i rispettivi processori di dati e l'enclave sottostante hanno accesso ai dati personali in chiaro. L'unico luogo in cui i dati sono esposti, al di fuori degli ambienti dei rispettivi processori di dati, è nell'enclave stessa, progettata per impedire l'accesso e la manomissione.

AWS PrivateLink

Molte organizzazioni vogliono limitare l'esposizione dei dati personali a reti non affidabili. Ad esempio, se si desidera migliorare la privacy della progettazione complessiva dell'architettura applicativa, è possibile segmentare le reti in base alla sensibilità dei dati (in modo analogo alla separazione logica e fisica dei set di dati descritta nella Servizi e funzionalità AWS che aiutano a segmentare i dati sezione). AWS PrivateLinkti aiuta a creare connessioni private unidirezionali dai tuoi cloud privati virtuali (VPCs) a servizi esterni al VPC. Utilizzando AWS PrivateLink, è possibile configurare connessioni private dedicate ai servizi che archiviano o elaborano dati personali nel proprio ambiente; non è necessario connettersi a endpoint pubblici e trasferire questi dati su reti pubbliche non affidabili. Quando si abilitano gli endpoint di AWS PrivateLink servizio per i servizi inclusi, non è necessario un gateway Internet, un dispositivo NAT, un indirizzo IP pubblico, una connessione o

AWS Direct Connect AWS Site-to-Site VPN una connessione per comunicare. Quando si utilizza AWS PrivateLink per connettersi a un servizio che fornisce l'accesso ai dati personali, è possibile utilizzare le policy degli endpoint VPC e i gruppi di sicurezza per controllare l'accesso, in base alla definizione del perimetro dei dati dell'organizzazione. Per un esempio di policy sugli endpoint VPC che consente solo ai principi e AWS alle risorse IAM di un'organizzazione affidabile di accedere a un endpoint di servizio, consulta Richiedi l'iscrizione all'organizzazione per accedere alle risorse VPC questa guida.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) ti aiuta a condividere in modo sicuro le tue risorse Account AWS per ridurre il sovraccarico operativo e fornire visibilità e verificabilità. Mentre pianifichi la tua strategia di segmentazione multi-account, valuta la possibilità di AWS RAM condividere gli archivi di dati personali archiviati in un account separato e isolato. Puoi condividere tali dati personali con altri account affidabili ai fini del trattamento. In AWS RAM, puoi gestire le autorizzazioni che definiscono quali azioni possono essere eseguite su risorse condivise. Tutte le chiamate API a AWS RAM sono registrate. CloudTrail Inoltre, puoi configurare Amazon CloudWatch Events in modo che ti invii automaticamente notifiche per eventi specifici in AWS RAM, ad esempio quando vengono apportate modifiche a una condivisione di risorse.

Sebbene sia possibile condividere molti tipi di AWS risorse con altri utenti Account AWS utilizzando policy basate su risorse in IAM o bucket policy in Amazon S3, AWS RAM offre diversi vantaggi aggiuntivi per la privacy. AWS offre ai proprietari dei dati una visibilità aggiuntiva su come e con chi i dati vengono condivisi tra di loro, tra cui: Account AWS

- Poter condividere una risorsa con un'intera unità organizzativa anziché aggiornare manualmente gli elenchi di account IDs
- Applicazione della procedura di invito per l'avvio della condivisione se l'account consumatore non fa parte dell'organizzazione
- Visibilità su quali responsabili IAM specifici hanno accesso a ogni singola risorsa

Se in precedenza hai utilizzato una policy basata sulle risorse per gestire una condivisione di risorse e desideri utilizzarla al suo AWS RAM posto, utilizza l'operazione API. PromoteResourceShareCreatedFromPolicy

Amazon SageMaker AI

Amazon SageMaker AI è un servizio di machine learning (ML) gestito che ti aiuta a creare e addestrare modelli di machine learning per poi distribuirli in un ambiente ospitato pronto per la produzione. SageMaker L'intelligenza artificiale è progettata per semplificare la preparazione dei dati di addestramento e la creazione di funzionalità del modello.

Monitoraggio del modello Amazon SageMaker AI

Molte organizzazioni considerano la deriva dei dati durante l'addestramento dei modelli di machine learning. La deriva dei dati è 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 di machine learning. Se la natura statistica dei dati che un modello di machine learning riceve durante la produzione si discosta dalla natura dei dati di base su cui è stato addestrato, l'accuratezza delle previsioni potrebbe diminuire. Amazon SageMaker AI Model Monitor può monitorare continuamente la qualità dei modelli di machine learning di Amazon SageMaker AI in produzione e monitorare la qualità dei dati. Il rilevamento precoce e proattivo della deriva dei dati può aiutarti a implementare azioni correttive, come la riqualificazione dei modelli, il controllo dei sistemi a monte o la risoluzione di problemi di qualità dei dati. Model Monitor può ridurre la necessità di monitorare manualmente i modelli o creare strumenti aggiuntivi.

Amazon SageMaker AI Clarify

Amazon SageMaker AI Clarify fornisce informazioni sulla distorsione e sulla spiegabilità del modello. SageMaker AI Clarify è comunemente usato durante la preparazione dei dati dei modelli ML e la fase di sviluppo generale. Gli sviluppatori possono specificare gli attributi di interesse, come il sesso o l'età, e SageMaker AI Clarify esegue una serie di algoritmi per rilevare qualsiasi presenza di distorsioni in tali attributi. Dopo l'esecuzione dell'algoritmo, SageMaker AI Clarify fornisce un report visivo con una descrizione delle fonti e delle misurazioni dei possibili pregiudizi in modo da poter identificare i passaggi per rimediare al pregiudizio. Ad esempio, in un set di dati finanziari che contiene solo alcuni esempi di prestiti commerciali concessi a una fascia di età rispetto ad altre, è SageMaker possibile segnalare gli squilibri in modo da evitare un modello che sfavorisce quella fascia di età. È inoltre possibile verificare la presenza di pregiudizi nei modelli già addestrati esaminandone le previsioni e monitorando continuamente l'eventuale presenza di pregiudizi nei modelli di machine learning. Infine, SageMaker AI Clarify è integrato con Amazon SageMaker AI Experiments per fornire un grafico che spiega quali funzionalità hanno contribuito maggiormente al processo di previsione complessivo di un modello. Queste informazioni potrebbero essere utili per

raggiungere i risultati di spiegabilità e potrebbero aiutarti a determinare se un particolare input del modello ha più influenza di quanto dovrebbe sul comportamento generale del modello.

SageMaker Scheda modello Amazon

Amazon SageMaker Model Card può aiutarti a documentare dettagli critici sui tuoi modelli di machine learning per scopi di governance e reporting. Questi dettagli possono includere il proprietario del modello, lo scopo generale, i casi d'uso previsti, le ipotesi formulate, la valutazione del rischio di un modello, i dettagli e le metriche della formazione e i risultati della valutazione. Per ulteriori informazioni, vedere Model Explainability with AWS Artificial Intelligence and Machine Learning Solutions (AWS white paper).

AWS funzionalità che aiutano a gestire il ciclo di vita dei dati

Quando i dati personali non sono più necessari, puoi utilizzare il ciclo di vita e le time-to-live policy per i dati in molti archivi di dati diversi. Quando configuri le politiche di conservazione dei dati, considera le seguenti posizioni che potrebbero contenere dati personali:

- Database, come Amazon DynamoDB e Amazon Relational Database Service (Amazon RDS)
- Bucket Amazon S3
- Registri da e CloudWatch CloudTrail
- Dati memorizzati nella cache provenienti da migrazioni in AWS Database Migration Service ()AWS DMS e progetti AWS Glue DataBrew
- Backup e istantanee

Le seguenti Servizi AWS funzionalità possono aiutarti a configurare le politiche di conservazione dei dati nei tuoi AWS ambienti:

- Ciclo di vita di Amazon S3: un insieme di regole che definiscono le azioni che Amazon S3 applica a un gruppo di oggetti. Nella configurazione Amazon S3 Lifecyle, puoi creare azioni di scadenza, che definiscono quando Amazon S3 elimina gli oggetti scaduti per tuo conto. Per ulteriori informazioni, consulta Gestione del ciclo di vita dell’archiviazione.
- Amazon Data Lifecycle Manager: in Amazon EC2, crea una policy che automatizzi la creazione, la conservazione e l'eliminazione di snapshot di Amazon Elastic Block Store (Amazon EBS) e Amazon Machine Images () supportate da EBS. AMIs

- DynamoDB Time to Live (TTL): definisce un timestamp per elemento che determina quando un elemento non è più necessario. Poco dopo la data e l'ora del timestamp specificato, DynamoDB elimina l'elemento dalla tabella.
- Impostazioni di conservazione dei log nei CloudWatch log: è possibile regolare la politica di conservazione per ogni gruppo di log su un valore compreso tra 1 giorno e 10 anni.
- AWS Backup— Implementazione centralizzata di policy di protezione dei dati per configurare, gestire e governare l'attività di backup su una varietà di AWS risorse, tra cui bucket S3, istanze di database RDS, tabelle DynamoDB, volumi EBS e molte altre. Applica le policy di backup alle tue AWS risorse specificando i tipi di risorse o fornisci ulteriore granularità applicando in base ai tag di risorsa esistenti. Verifica e crea report sulle attività di backup da una console centralizzata per contribuire a soddisfare i requisiti di conformità del backup.

Servizi e funzionalità AWS che aiutano a segmentare i dati

La segmentazione dei dati è il processo mediante il quale si archiviano i dati in contenitori separati. Questo può aiutarvi a fornire misure di sicurezza e autenticazione differenziate per ogni set di dati e a ridurre l'ambito di impatto dell'esposizione per l'intero set di dati. Ad esempio, anziché archiviare tutti i dati dei clienti in un unico database di grandi dimensioni, è possibile segmentarli in gruppi più piccoli e più gestibili.

Puoi utilizzare la separazione fisica e logica per segmentare i dati personali:

- Separazione fisica: l'atto di archiviare i dati in archivi di dati separati o di distribuirli in AWS risorse separate. Sebbene i dati siano fisicamente separati, entrambe le risorse potrebbero essere accessibili agli stessi responsabili. Questo è il motivo per cui consigliamo di combinare la separazione fisica con la separazione logica.
- Separazione logica: l'atto di isolare i dati utilizzando i controlli di accesso. Diverse funzioni lavorative richiedono diversi livelli di accesso a sottoinsiemi di dati personali. Per un esempio di policy che implementa la separazione logica, consulta questa Concedi l'accesso a specifici attributi di Amazon DynamoDB guida.

La combinazione di separazione logica e fisica offre flessibilità, semplicità e granularità nella stesura di politiche basate sull'identità e sulle risorse per supportare l'accesso differenziato tra le funzioni lavorative. Ad esempio, può essere complesso dal punto di vista operativo creare le policy che separano logicamente diverse classificazioni dei dati in un unico bucket S3. L'utilizzo di bucket S3 dedicati per ogni classificazione dei dati semplifica la configurazione e la gestione delle policy.

Esempi di politiche relative alla privacy

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Molte organizzazioni che gestiscono dati sensibili adottano un approccio preventivo, con livelli di controlli investigativi e reattivi implementati ovunque. Questa sezione fornisce esempi di politiche relative alla privacy per AWS Identity and Access Management (IAM) e (). AWS Organizations AWS Key Management Service AWS KMS Queste politiche possono aiutare l'organizzazione a soddisfare vari obiettivi di privacy in materia di utilizzo, limitazione della divulgazione e trasferimento transfrontaliero dei dati utilizzando un approccio preventivo. Molte di queste politiche sono citate nelle sezioni precedenti di questa guida.

Questa sezione contiene le seguenti politiche di esempio:

- Richiedi l'accesso da indirizzi IP specifici
- Richiedi l'iscrizione all'organizzazione per accedere alle risorse VPC
- Limita i trasferimenti di dati tra Regioni AWS
- Concedi l'accesso a specifici attributi di Amazon DynamoDB
- Limita le modifiche alle configurazioni VPC
- Richiedi l'attestazione per utilizzare una chiave AWS KMS

Richiedi l'accesso da indirizzi IP specifici

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Questa policy consente all'`john_stiles`utente di assumere ruoli IAM solo se la chiamata proviene da un indirizzo IP compreso negli intervalli `192.0.2.0/24` o`203.0.113.0/24`. Questa politica può aiutare a prevenire la divulgazione involontaria di dati personali e i trasferimenti di dati transfrontalieri indesiderati. Ad esempio, se la tua organizzazione dispone di personale di assistenza clienti che richiede l'accesso ai dati personali, potresti volere che il personale di supporto acceda a tali dati solo dagli uffici che si trovano in un sottoinsieme specifico. Regioni AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

Richiedi l'iscrizione all'organizzazione per accedere alle risorse VPC

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Questa policy sugli endpoint VPC consente solo ai principali AWS Identity and Access Management (IAM) e alle risorse `o-1abcde123` dell'organizzazione di accedere agli endpoint Amazon Personalize (Amazon S3). Questo controllo preventivo aiuta a stabilire una zona di fiducia e a definire il perimetro

dei dati personali. Per ulteriori informazioni su come questa politica può contribuire a proteggere la privacy e i dati personali nell'organizzazione, consulta AWS PrivateLink questa guida.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyIntendedResourcesAndPrincipals",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-1abcde123",
                    "aws:ResourceOrgID": "o-1abcde123"
                }
            }
        }
    ]
}
```

Limita i trasferimenti di dati tra Regioni AWS

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Ad eccezione di due ruoli AWS Identity and Access Management (IAM), questa politica di controllo del servizio nega le chiamate API a destinatari regionali Servizi AWS Regioni AWS diversi da `eu-west-1` e `eu-central-1`. Questo SCP può aiutare a prevenire la creazione di servizi di AWS archiviazione ed elaborazione in regioni non approvate. Questo può aiutare a evitare che i dati personali vengano gestiti del tutto Servizi AWS in quelle regioni. Questa policy utilizza un `NotAction` parametro perché tiene conto dei servizi AWS globali, come IAM, e dei servizi che si integrano con i servizi globali, come AWS Key Management Service (AWS KMS) e Amazon CloudFront. Nei valori dei parametri, puoi specificare i servizi globali e altri servizi non applicabili come eccezioni. Per ulteriori informazioni su come questa politica può contribuire a proteggere la privacy e i dati personali nell'organizzazione, consulta AWS Organizations questa guida.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
```

```
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Concedi l'accesso a specifici attributi di Amazon DynamoDB

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Mentre la tua organizzazione discute delle strategie per separare fisicamente e logicamente i dati personali, valuta quali servizi di AWS storage supportano politiche di controllo degli accessi granulari in (IAM). AWS Identity and Access Management La seguente politica basata sull'identità consente il recupero solo degli attributi `UserID`, `SignUpTime`, e da `LastLoggedIn` una tabella Amazon DynamoDB denominata. `Users` Ad esempio, potresti associare questa policy a un ruolo di assistenza clienti anziché concedere a questo ruolo l'accesso all'intero set di dati personali. Per ulteriori informazioni su come questa politica può contribuire a proteggere la privacy e i dati personali

nell'organizzazione, consulta Servizi e funzionalità AWS che aiutano a segmentare i dati questa guida.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan",
            "dynamodb:TransactGetItems"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
                  "SignUpTime",
                  "LastLoggedIn"
               ]
            },
            "StringEquals":{
               "dynanamodb:Select":[
                  "SPECIFIC_ATTRIBUTES"
               ]
            }
         }
      }
   ]
}
```

Limita le modifiche alle configurazioni VPC

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Dopo aver progettato e implementato l' AWS infrastruttura che supporta i requisiti di trasferimento transfrontaliero dei dati, che include i flussi di dati di rete, potresti voler prevenire le modifiche. La seguente politica di controllo del servizio aiuta a prevenire la deriva o la modifica involontaria della configurazione del VPC. Nega nuovi allegati gateway Internet, connessioni peering VPC, allegati gateway di transito e nuove connessioni VPN. Per ulteriori informazioni su come questa politica può aiutare a proteggere la privacy e i dati personali nell'organizzazione, consulta questa guida. AWS Transit Gateway

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:AttachEgressOnlyInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
                "ec2:CreateRouteTable",
                "ec2:CreateRoute",
                "ec2:AssociateRouteTable",
                "ec2:ModifyVpcAttribute",
                "ec2:*TransitGateway",
                "ec2:*TransitGateway*",
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"

            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
```

```
}
```

Richiedi l'attestazione per utilizzare una chiave AWS KMS

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

La seguente politica chiave AWS Key Management Service (AWS KMS) consente alle istanze di AWS Nitro Enclave di utilizzare una chiave KMS solo se il documento di attestazione dell'enclave contenuto nella richiesta corrisponde alle misurazioni nella dichiarazione delle condizioni. Questa politica consente solo alle enclave affidabili di decrittografare i dati. Per ulteriori informazioni su come questa politica può contribuire a proteggere la privacy e i dati personali nell'organizzazione, consulta AWS Enclavi Nitro questa guida. Per un elenco completo delle chiavi di AWS KMS condizione che possono essere utilizzate nelle politiche chiave e nelle politiche AWS Identity and Access Management (IAM), consulta Condition keys for AWS KMS.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Enable enclave data processing",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:role/data-processing"
         },
         "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey",
            "kms:GenerateRandom"
         ],
         "Resource": "*",
         "Condition": {
            "StringEqualsIgnoreCase": {
               "kms:RecipientAttestation:ImageSha384":
 "EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdEXAMPLE",
               "kms:RecipientAttestation:PCR0":
 "EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfdd36c08b2c79552928702EXAM
               "kms:RecipientAttestation:PCR1":
 "EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbecc2eec1bf0b4ae749d311c663f464cde9f718aEXAM
```

```
                "kms:RecipientAttestation:PCR2":
  "EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM
                "kms:RecipientAttestation:PCR3":
  "EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM
                "kms:RecipientAttestation:PCR4":
  "EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM
                "kms:RecipientAttestation:PCR8":
  "EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM
            }
          }
        }
    ]
}
```

Risorse

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

AWS Guida prescrittiva

- AWS Architettura di riferimento per la sicurezza (AWS SRA)

AWS documentazione

- Protezione dei dati (AWS Well-Architected Framework)
- Classificazione dei dati (white paper)AWS
- Amazon Web Services: rischio e conformità (AWS white paper)
- Architetture ibride per soddisfare i requisiti di elaborazione dei dati personali (white paper)AWS
- Come orientarsi verso la conformità al GDPR su (white paper) AWSAWS
- Creazione di un perimetro di dati su (white paper) AWSAWS
- AWS Documentazione sulla sicurezza

Altre AWS risorse

- AWS Programmi di conformità
- AWS Modello di responsabilità condivisa
- Domande frequenti sulla privacy dei dati
- AWS Servizi di garanzia della sicurezza
- AWS Digital Sovereignty Pledge: controllo senza compromessi (post sul blog)AWS
- AWS Apprendimento sulla sicurezza

Collaboratori

Ci piacerebbe sentire la tua opinione. Fornisci un feedback sul AWS PRA rispondendo a un breve sondaggio.

Questa guida è stata redatta dal team di AWS Security Assurance Services. Per ricevere assistenza nell'implementazione delle raccomandazioni contenute in questa guida e nell'operatività dei carichi di lavoro, contatta il team dei Security Assurance Services.AWS

Autori principali

- Daniel Nieters, consulente principale per la privacy AWS
- Amber Welch, consulente senior in materia di privacy AWS
- Robert Carter, responsabile tecnico del programma AWS

Collaboratori

- Avik Mukherjee, consulente senior per la sicurezza AWS
- David Bounds, architetto senior delle soluzioni AWS
- Jeff Lombardo, AWS architetto senior delle soluzioni di sicurezza
- Ram Ramani, AWS principale architetto delle soluzioni di sicurezza
- Vanessa Jacobs, consulente senior per la sicurezza 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
Aggiornamenti significativi	Abbiamo apportato aggiornamenti significativi dappertutto.	26 marzo 2024
Pubblicazione iniziale	—	2 ottobre 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 database Oracle locale su Oracle su un'istanza in. EC2 Cloud AWS
- Trasferire (eseguire il rehosting a livello hypervisor): trasferisci l'infrastruttura sul cloud senza acquistare nuovo hardware, riscrivere le applicazioni o modificare le operazioni esistenti. Si esegue la migrazione dei server da una piattaforma locale a un servizio cloud per la stessa piattaforma. Esempio: migra un'applicazione suMicrosoft Hyper-V. AWS
- Riesaminare (mantenere): mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a un momento successivo e applicazioni legacy che desideri mantenere, perché non vi è alcuna giustificazione aziendale per effettuarne la migrazione.
- Ritirare: disattiva o rimuovi le applicazioni che non sono più necessarie nell'ambiente di origine.

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

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

migrazione attiva-passiva

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

funzione aggregata

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

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

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

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

AWS Workload Qualification Framework (WQF)AWS

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

B

bot difettoso

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

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

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

Classificazione binaria

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

filtro Bloom

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

distribuzioni blu/verdi

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

bot

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

botnet

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

ramo

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

accesso break-glass

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

strategia brownfield

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

cache del buffer

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

capacità di business

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

pianificazione della continuità operativa (BCP)

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

C

CAF

Vedi AWS Cloud Adoption Framework.

implementazione canaria

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

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

Centro di eccellenza cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

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

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

CMDB

Vedi database di gestione della configurazione.

repository di codice

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

cache fredda

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

dati freddi

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

visione artificiale (CV)

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

deriva della configurazione

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

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

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

CV

Vedi visione artificiale.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

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

deriva dei dati

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

dati in transito

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

rete di dati

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di definizione del database.

deep ensemble

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

deep learning

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

defense-in-depth

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

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

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

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

gemello digitale

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

tabella delle dimensioni

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

disastro

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

disaster recovery (DR)

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

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

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

DOTT.

Vedi disaster recovery.

rilevamento della deriva

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

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

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

scambio elettronico di dati (EDI)

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

crittografia

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

chiave crittografica

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

endianità

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

endpoint

Vedi service endpoint.

servizio endpoint

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

pianificazione delle risorse aziendali (ERP)

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

crittografia envelope

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

ambiente

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

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

epica

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

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

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

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

F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

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

prompt con pochi scatti

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

Vedi il modello di base.

modello di fondazione (FM)

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

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

G

AI generativa

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

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

immagine dorata

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

strategia greenfield

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

guardrail

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

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

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

alta disponibilità (HA)

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

modernizzazione storica

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

dati di esclusione

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

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

I

IaC

Considera l'infrastruttura come codice.

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

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

VPC in ingresso (ingress)

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

migrazione incrementale

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

IIoInternet delle cose industriale (T)

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

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

modello linguistico di grandi dimensioni (LLM)

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

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

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

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

ramo principale

Vedi filiale.

malware

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

servizi gestiti

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

sistema di esecuzione della produzione (MES)

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

MAP

Vedi Migration Acceleration Program.

meccanismo

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

account membro

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

MEH.

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

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

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

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

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

migrazione su larga scala

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

fabbrica di migrazione

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

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

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

Vedi machine learning.

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

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

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

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

infrastruttura mutabile

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

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

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

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

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

OPC-UA

Vedi Open Process Communications - Unified Architecture.

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

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

tecnologia operativa (OT)

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

integrazione delle operazioni (OI)

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

trail organizzativo

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

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

gestione del cambiamento organizzativo (OCM)

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

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

ORR

Vedi la revisione della prontezza operativa.

- NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

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

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

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

persistenza poliglotta

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

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

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

concatenamento rapido

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

pseudonimizzazione

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

publish/subscribe (pub/sub)

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

Q

Piano di query

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

regressione del piano di query

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

R

Matrice RACI

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

STRACCIO

Vedi Retrieval Augmented Generation.

ransomware

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

Matrice RASCI

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

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

Regione

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

regressione

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

riospitare

Vedi 7 R.

rilascio

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

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

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

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi l'obiettivo del punto di ripristino.

RTO

Vedi l'obiettivo del tempo di ripristino.

runbook

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

S

SAML 2.0

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

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

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

sicurezza fin dalla progettazione

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

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

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

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

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

Modello di responsabilità condivisa

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

SIEM

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

punto di errore singolo (SPOF)

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

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

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

SPOF

Vedi punto di errore singolo.

schema a stella

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

modello del fico strangolatore

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

sottorete

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

controllo di supervisione e acquisizione dati (SCADA)

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

crittografia simmetrica

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

test sintetici

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

prompt di sistema

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

T

tags

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

variabile di destinazione

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

elenco di attività

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

Ambiente di test

Vedi ambiente.

training

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

Transit Gateway

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

flusso di lavoro basato su trunk

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

Accesso attendibile

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

regolazione

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

team da due pizze

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

U

incertezza

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

compiti indifferenziati

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

ambienti superiori

Vedi ambiente.

V

vacuum

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

controllo delle versioni

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

Peering VPC

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

vulnerabilità

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

W

cache calda

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

dati caldi

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

funzione finestra

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

Carico di lavoro

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

flusso di lavoro

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

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

Z

exploit zero-day

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

vulnerabilità zero-day

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

prompt zero-shot

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

applicazione zombie

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

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