Architettura di cloud computing sicura AWS per il Dipartimento della Difesa degli Stati Uniti

AWS Guida prescrittiva

AWS Guida prescrittiva: Architettura di cloud computing sicura AWS per il Dipartimento della Difesa degli Stati Uniti

Table of Contents

Architettura di cloud computing sicura AWS per il Dipartimento della Difesa degli Stati Uniti

Rob Higareda e Rughved Gadgil, Amazon Web Services ()AWS

Marzo 2024 (storia del documento)

Il Dipartimento della Difesa degli Stati Uniti (DoD) segmenta le informazioni sul cloud in livelli di impatto (). ILs Il livello di impatto è associato alla sensibilità delle informazioni e al rischio di perdita della riservatezza, dell'integrità o della disponibilità di tali informazioni. IL4contiene informazioni non classificate controllate dal DoD CUI () e IL5 ospita informazioni CUI DoD e National Security Systems (). NSS Questa guida è progettata per aiutarti a costruire una landing zone con supporti IL4 e IL5 informazioni.

Per creare un'infrastruttura cloud IL4 conforme o IL5 conforme, devi creare componenti specifici. La Defense Information Systems Agency (DISA) Secure Cloud Computing Architecture (SCCA) è una selezione di servizi di sicurezza e gestione del cloud. Fornisce un approccio standardizzato per la creazione di un confine cloud. Include SCCA anche componenti di sicurezza a livello di applicazione IL4 e IL5 informazioni ospitate nel cloud.

Questa guida ti aiuta a soddisfare SCCA i requisiti utilizzando Landing Zone Accelerator () su. LZA AWS La LZA soluzione implementa un set di funzionalità di base progettato per allinearsi con le AWS migliori pratiche e diversi framework di conformità globali. LZAPossono aiutarti a creare molti dei componenti necessari per aderire al DoD. SCCA Questa guida consiglia inoltre come aggiungere componenti aggiuntivi per la SCCA conformità e stabilire una base sicura per i propri ambienti cloud. AWS Sebbene questa guida non includa tutte le situazioni potenziali, fornisce indicazioni su come iniziare e su quali Servizi AWS possono aiutarti a soddisfare SCCA i requisiti.

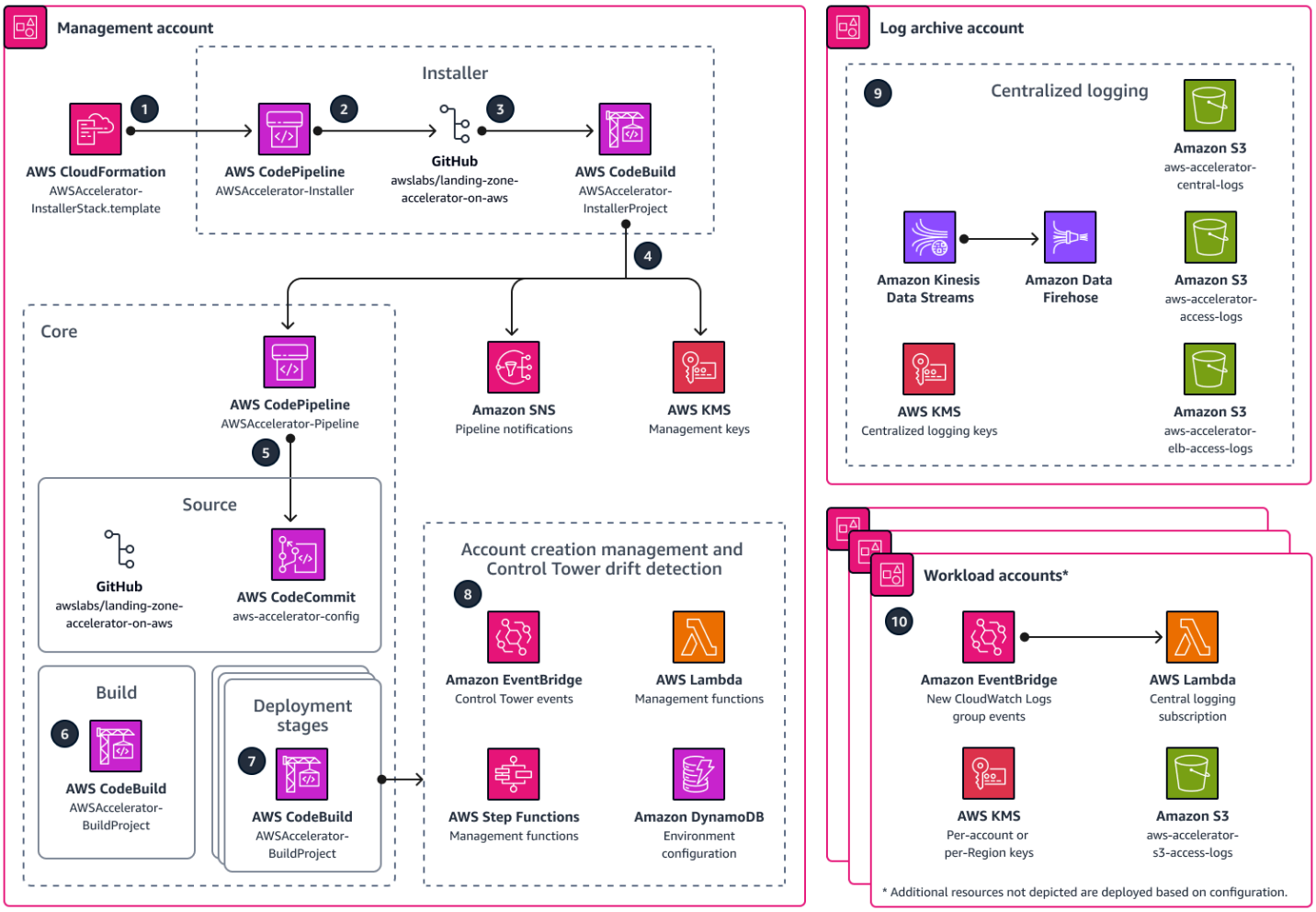
Destinatari principali

Questa guida è destinata alle persone che devono conformarsi all'architettura DoD Secure Cloud Computing per proteggere IL4 le IL5 informazioni in. Cloud AWS Se non l'hai già fatto, consulta la Guida ai requisiti di sicurezza del DISA cloud computing prima di leggere questa guida.

Panoramica del Landing Zone Accelerator

Per costruire una landing zone conforme alla Defense Information Systems Agency (DISA) Secure Cloud Computing Architecture (SCCA), è necessario disporre di alcuni elementi che consentano di soddisfare i requisiti minimi. AWS AWS ha creato Landing Zone Accelerator (LZA) per aiutarti a implementare una landing zone conforme ai requisiti necessari. Utilizzando la LZA soluzione, è possibile distribuire l'ambiente utilizzando un set di file di configurazione. Questi file di configurazione consentono di concentrarsi sulla fornitura di un ambiente anziché sull'apprendimento individuale Servizio AWS e su come implementarlo.

L'immagine seguente mostra i servizi coinvolti nella LZA distribuzione. I numeri indicano il flusso di lavoro, dalla modifica dei file di configurazione alla configurazione degli Servizi AWS account del carico di lavoro.



Questa soluzione è progettata per allinearsi alle AWS migliori pratiche e conformarsi a diversi framework di conformità globali. Se utilizzata in coordinamento con servizi come AWS Control Tower, questa soluzione fornisce una soluzione completa e low-code con più di 35 funzionalità. Servizi AWS In particolare, questa soluzione consente di gestire e governare un ambiente multi-account progettato per supportare carichi di lavoro altamente regolamentati e requisiti di conformità complessi. LZAti aiuta a stabilire la disponibilità della piattaforma con funzionalità di sicurezza, conformità e operative. Questa guida include note specifiche sull'uso di questa soluzione per supportare l'allineamento alle linee guida della Federazione e del Dipartimento della Difesa (DoD) degli Stati Uniti d'America (USA).

AWS fornisce la LZA soluzione come progetto open source che è stato creato utilizzando. AWS Cloud Development Kit (AWS CDK) È possibile installarlo direttamente nel proprio ambiente, ottenendo l'accesso completo alla soluzione Infrastructure as Code (IaC).

Tramite un set semplificato di file di configurazione, è possibile:

- Configurare funzionalità, guardrail e servizi di sicurezza aggiuntivi, come regole AWS Configgestite e. AWS Security Hub
- Gestisci la topologia di rete di base tramite servizi come Amazon Virtual Private Cloud VPC (Amazon) e AWS Transit Gateway. AWS Network Firewall
- Genera account di carico di lavoro aggiuntivi utilizzando Account Factory.AWS Control Tower

Non sono richiesti costi aggiuntivi o impegni anticipati per utilizzare Landing Zone Accelerator su. AWS Paghi solo Servizi AWS quello che attivi per configurare la piattaforma e far funzionare i guardrail. Questa soluzione può supportare anche AWS partizioni non standard, incluse le AWS GovCloud (US) regioni Secret e AWS AWS Top Secret.

> **Important**
>
> La LZA soluzione, di per sé, non ti rende conforme. Fornisce l'infrastruttura di base da cui è possibile integrare soluzioni complementari aggiuntive. Le informazioni contenute nella guida all'LZAimplementazione non sono esaustive. È necessario esaminare, valutare, valutare e approvare la soluzione in conformità con le caratteristiche, gli strumenti e le configurazioni di sicurezza particolari dell'organizzazione. È responsabilità esclusiva dell'utente e della sua organizzazione determinare quali requisiti normativi siano applicabili e garantire la conformità a tutti i requisiti. Sebbene questa soluzione descriva sia i requisiti tecnici che quelli amministrativi, non aiuta a rispettare i requisiti amministrativi non tecnici.

Pianificazione della distribuzione su LZA AWS

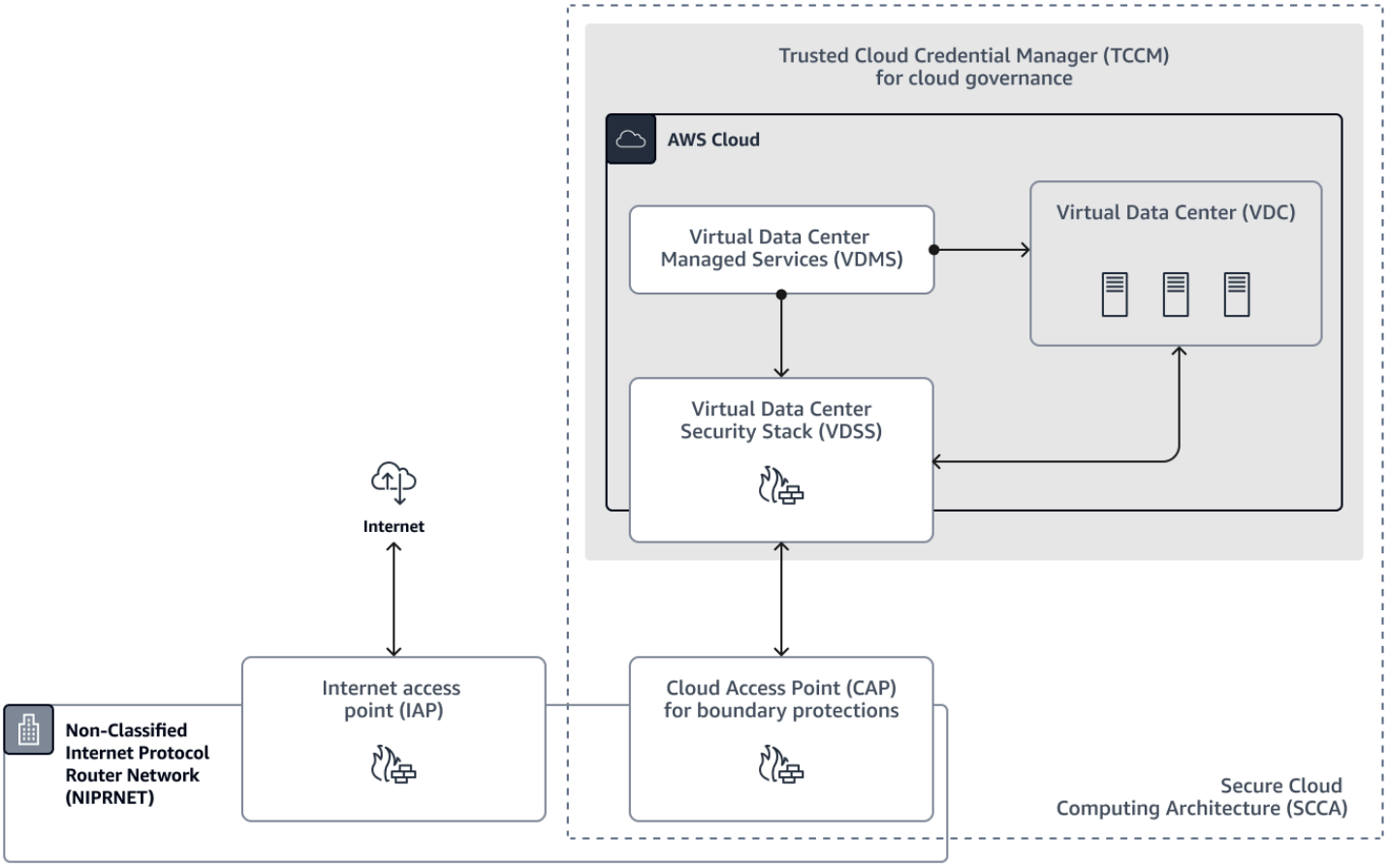
AWS ha creato una guida all'implementazione dettagliata per l'implementazione della soluzione Landing Zone Accelerator (LZA) su. AWS Per un diagramma di architettura e una panoramica delle fasi di implementazione, consulta Diagramma di architettura nella Landing Zone Accelerator on Implementation Guide. AWS L'ambiente deve soddisfare i prerequisiti prima di implementare la soluzione. Utilizzando i requisiti nel capitolo SCCA Componenti e requisiti di questa guida, è possibile scegliere tra le opzioni di distribuzione descritte nella guida all'LZAimplementazione.

SCCAcomponenti e requisiti

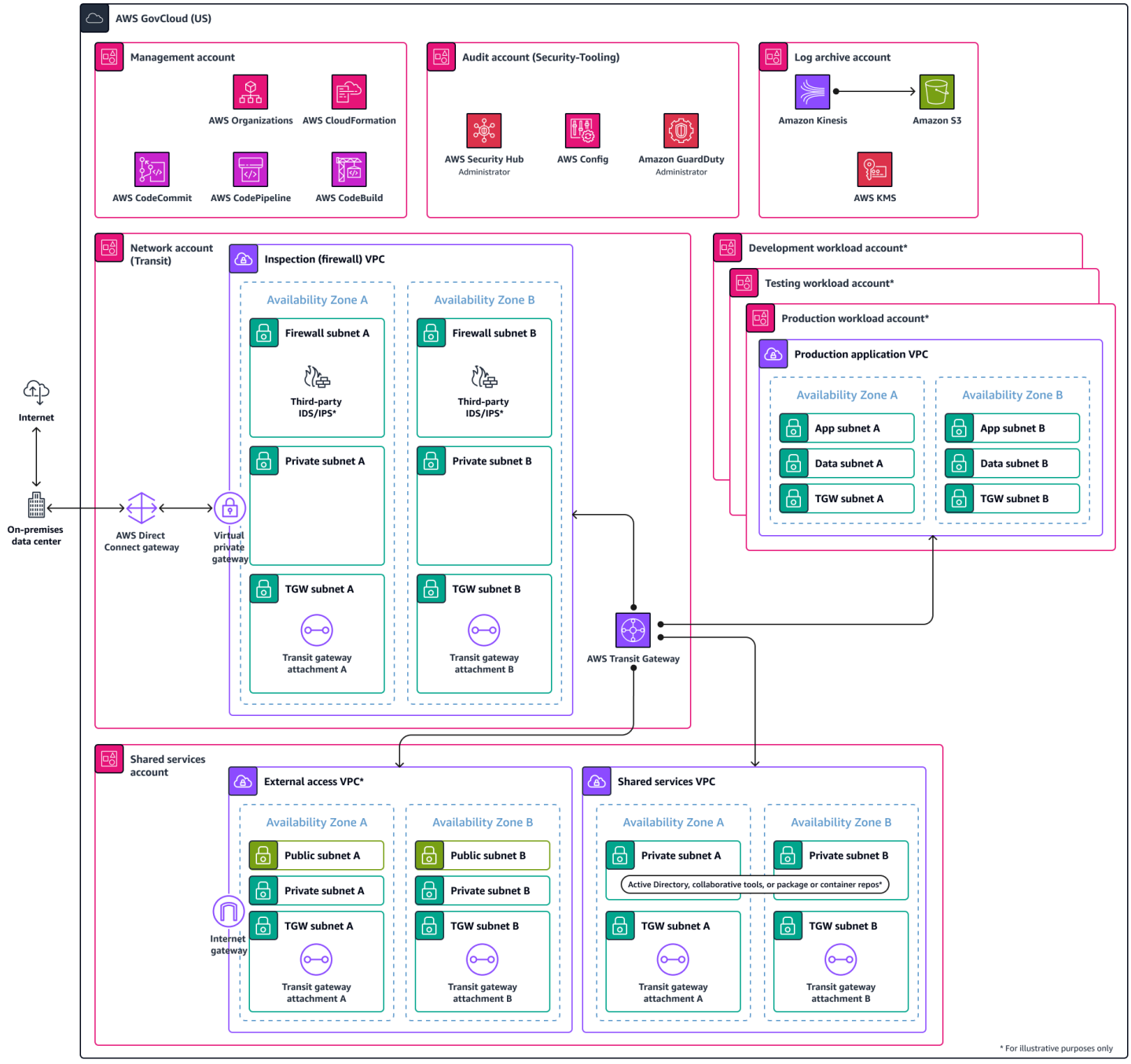
La Defense Information Systems Agency (DISA) Secure Cloud Computing Architecture (SCCA), adottata dal Dipartimento della Difesa degli Stati Uniti (DoD), è pensata per essere un approccio scalabile ed economico per proteggere le applicazioni basate sul cloud nell'ambito di un'architettura di sicurezza comune. Fornisce un approccio standard per la protezione e i dati negli ambienti cloud. IL4 IL5 Come descritto nella scheda DISA SCCA informativa, i componenti generali di includono: SCCA

- Cloud Access Point (CAP): fornisce l'accesso al cloud e protegge le reti DoD dal cloud. Protezioni semplificate incentrate sulla protezione dei confini della rete.
- Virtual Data Center Security Stack (VDSS): sicurezza dell'enclave di rete virtuale per proteggere applicazioni e dati nelle offerte cloud commerciali.
- Virtual Data Center Managed Services (VDMS): sicurezza dell'host delle applicazioni per l'accesso privilegiato degli utenti in ambienti commerciali.
- Trusted Cloud Credential Manager (TCCM): gestore di credenziali cloud per applicare il controllo degli accessi basato sui ruoli () e l'accesso con privilegi minimi. RBAC

L'immagine seguente mostra questi componenti di. SCCA



Questa sezione illustra in dettaglio ogni componente e i componenti corrispondenti LZA che possono aiutarti ad aderire allo standard della Defense Information Systems Agency (DISA). L'immagine seguente mostra la struttura LZA multi-account che crea i componenti di. SCCA Cloud AWS Questa struttura LZA multi-account è una base che consente di ottenere un'architettura completamente conforme ai requisiti. DISA SCCA Per un esempio di architettura che consente di soddisfare pienamente i requisiti di conformità, consulta il diagramma SCCAon AWS GovCloud architecture.



Punto di accesso cloud

Il Boundary Cloud Access Point (BCAP) o Cloud Access Point (CAP) è predeterminato dalla tua organizzazione. Pertanto, non rientra nell'ambito di questa guida. CAPFornisce l'accesso agli ambienti cloud commerciali dal Defense Information Systems Network (DISN). Fornisce CAP inoltre protezione dei confini DISN dal cloud. Al DISN confine, include funzionalità di difesa informatica, come firewall, sistemi di rilevamento delle intrusioni () e sistemi di prevenzione delle intrusioni (IDS).

IPS È normale che le organizzazioni utilizzino il DoD Cloud Native Access Point Reference Design per l'accesso. AWS

Stack di sicurezza per data center virtuali

Lo scopo del Virtual Data Center Security Stack (VDSS) è proteggere le applicazioni DOD proprietarie della missione ospitate in. AWS VDSSFornisce un'enclave per i servizi di sicurezza. VDSSEsegue la maggior parte delle operazioni di sicurezza in. SCCA Questo componente contiene servizi di sicurezza e di rete, come connettività in entrata, controlli degli accessi e servizi di protezione perimetrale, inclusi firewall per applicazioni Web, DDOS protezione, bilanciamenti del carico e risorse di routing di rete. VDSSPossono risiedere nell'infrastruttura cloud o on-premise, nel tuo data center. AWS oppure i fornitori di terze parti possono fornire VDSS funzionalità tramite Infrastructure as a Service (IaaS) AWS o possono offrire tali funzionalità tramite soluzioni software as a service (SaaS). Per ulteriori informazioni suVDSS, consulta la Guida ai requisiti di sicurezza del cloud computing del DoD.

La tabella seguente contiene i requisiti minimi per. VDSS Spiega se LZA soddisfa ogni requisito e quali possono essere utilizzati per Servizi AWS soddisfarli.

ID	VDSSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.2.1	VDSSDevono mantenere la separazione virtuale di tutto il traffico di gestione, utente e dati.	AWS Network Firewall Elenco di controllo dell'accesso alla rete (ACL) Gruppi di sicurezza per interfacce di rete elastiche	Isolare VPCs	Coperto
2.1.2.2	VDSSDevono consentire l'uso della crittografia	Amazon VPC (crittografa il	Le migliori pratiche di	Coperto

ID	VDSSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
	per la segmentazione del traffico di gestione.	traffico tra le istanze)	crittografia per Amazon VPC	
2.1.2.3	VDSSDevono fornire una funzionalità di reverse proxy per gestire le richieste di accesso dai sistemi client.	N/D	Servire contenuti utilizzando un reverse proxy completamente gestito	Non coperto
2.1.2.4	VDSSDevono fornire la capacità di ispezionare e filtrare le conversazioni a livello di applicazione sulla base di un insieme predefinito di regole (tra cuiHTTP) l'identificazione e il blocco dei contenuti dannosi.	AWS WAF Network Firewall	Ispezione del corpo delle richieste Web TLSispezione del traffico con Network Firewall	Parzialmente coperto

ID	VDSSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.2.5	VDSSDevono fornire una capacità in grado di distinguere e bloccare il traffico non autorizzato a livello di applicazione.	AWS WAF	Come usare Amazon GuardDuty e AWS WAF bloccare automaticamente gli host sospetti	Non coperto
2.1.2.6	VDSSDevono fornire una capacità di monitoraggio delle attività della rete e del sistema per rilevare e segnalare le attività dannose relative al traffico in entrata e in uscita dalle reti/enclavi private virtuali del proprietario della missione.	Log di flusso VPC Amazon GuardDuty AWS Enclavi Nitro	AWS Laboratorio Nitro Enclaves	Parzialmente coperto

ID	VDSSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.2.7	VDSSDevono fornire una capacità di monitoraggio delle attività di rete e di sistema per fermare o bloccare le attività dannose rilevate.	Network Firewall AWS WAF	N/D	Parzialmente coperto
2.1.2.8	VDSSDeve ispezionare e filtrare il traffico che attraversa reti/enclavi private virtuali del titolare della missione.	Network Firewall	Implementa un filtraggio centralizzato del traffico	Coperto

ID	VDSSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.2.9	VDSSDeve eseguire l'interruzione e l'ispezione del traffico di SSL TLS comunicazione supportando l'autenticazione singola e doppia per il traffico destinato ai sistemi ospitati all'interno del. CSE	Network Firewall	Modelli di implementazione per Network Firewall	Coperto
2.1.2.10	VDSSDevono fornire un'interfaccia per condurre porti, protocolli e attività di gestione dei servizi (PPSM) al fine di fornire il controllo agli operatori. MCD	Network Firewall	Modelli di implementazione per Network Firewall	Coperto

ID	VDSSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.2.11	VDSSDevono fornire una capacità di monitoraggio che acquisisca file di registro e dati sugli eventi per l'analisi della sicurezza informatica.	Amazon CloudWatch AWS CloudTrail	Registrazione per la risposta agli incidenti di sicurezza	Coperto
2.1.2.12	VDSSForniscono o forniscono informazioni sulla sicurezza e dati sugli eventi a un sistema di archiviazione assegnato per la raccolta, l'archiviazione e l'accesso comuni ai registri degli eventi da parte degli utenti privilegiati che svolgono attività di confine e missione. CND	CloudWatch Registri Amazon	Sicurezza nei registri CloudWatch	Coperto

ID	VDSSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.2.13	VDSSFornirà un sistema di gestione delle chiavi di crittografia conforme a FIPS -140-2 per l'archiviazione delle credenziali della chiave di crittografia privata generate dal DoD e assegnate al server per l'accesso e l'uso da parte del Web Application Firewall (WAF) nell'esecuzione di SSL TLS /interruzione e ispezione di sessioni di comunicazione crittografate.	AWS Secrets Manager AWS Key Management Service(AWS KMS)	Migliora la sicurezza di CloudFront origine di Amazon con AWS WAF Secrets Manager AWS KMS gestione delle chiavi con FIPS 140-2	Non coperto

ID	VDSSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.2.14	VDSSDevono fornire la capacità di rilevare e identificare il dirottamento della sessione applicativa.	N/D	N/D	Non coperto
2.1.2.15	VDSSDovranno fornire un'DMZestensione DoD per supportare le applicazioni con accesso a Internet ()IFAs.	N/D	N/D	Non coperto
2.1.2.16	VDSSDevono fornire una capacità di acquisizione completa dei pacchetti (FPC) o una FPC capacità equivalente a un servizio cloud per la registrazione e l'interpretazione delle comunicazioni trasversali.	Network Firewall Log di flusso VPC	N/D	Coperto

ID	VDSSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.2.17	VDSSDevono fornire metriche e statistiche sul flusso di pacchetti di rete per tutte le comunicazioni in transito.	CloudWatch	Monitora il throughput di rete degli endpoint di interfaccia utilizzando VPC CloudWatch	Coperto
2.1.2.18	VDSSDevono provvedere all'ispezione del traffico in entrata e in uscita dalla rete privata virtuale del proprietario di ciascuna missione.	Network Firewall	Implementa un filtraggio centralizzato del traffico	Coperto

Ci sono alcuni componenti definiti dall'CAPutente e non trattati in questa guida, poiché ogni agenzia ha i propri CAP collegamenti con AWS. È possibile integrare i componenti di VDSS con il LZA per aiutare a ispezionare il traffico in AWS entrata. I servizi utilizzati LZA forniscono la scansione dei confini e del traffico interno per proteggere l'ambiente. Per continuare a creare unVDSS, ci sono alcuni componenti dell'infrastruttura aggiuntivi che non sono inclusi in. LZA

Utilizzando il cloud privato virtuale (VPCs), è possibile stabilire dei limiti in ciascuno di essi Account AWS per contribuire al rispetto degli SCCA standard. Questo non è configurato come parte del programmaVPCs, LZA perché l'indirizzamento IP e il routing sono componenti che è necessario configurare in base alle esigenze dell'infrastruttura. Puoi implementare componenti come Domain Name System Security Extensions (DNSSEC) in Amazon Route 53. Puoi anche aggiungere prodotti commerciali AWS WAF o di terze parti WAFs per aiutarti a raggiungere gli standard necessari.

Inoltre, per supportare il requisito 2.1.2.7 del DISASCCA, è possibile utilizzare un Network GuardDutyFirewall per proteggere e monitorare l'ambiente per il traffico dannoso.

Managed Services per data center virtuali

Lo scopo di Virtual Data Center Managed Services (VDMS) è fornire sicurezza dell'host e servizi di data center condivisi. Le funzioni di VDMS possono essere eseguite nell'hub dell'utente SCCA oppure il proprietario della missione può implementarne alcune parti autonomamente. Account AWS Questo componente può essere fornito all'interno AWS dell'ambiente. Per ulteriori informazioni suVDMS, consulta la Guida ai requisiti di sicurezza del cloud computing del DoD.

La tabella seguente contiene i requisiti minimi per. VDMS Spiega se LZA soddisfa ogni requisito e quali possono essere utilizzati per Servizi AWS soddisfarli.

ID	VDMSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.3.1	VDMSDevono fornire una soluzione Assured Compliance Assessment (ACAS), o una soluzione equivalente approvata, per condurre il monitoraggio continuo di tutte le enclavi all'interno del. CSE	AWS Config AWS Security Hub AWS Audit Manager Amazon Inspector	Scansione delle vulnerabilità con Amazon Inspector	Parzialmente coperto
2.1.3.2	VDMSDevono fornire un sistema di sicurezza basato	N/D	N/D	Non coperto

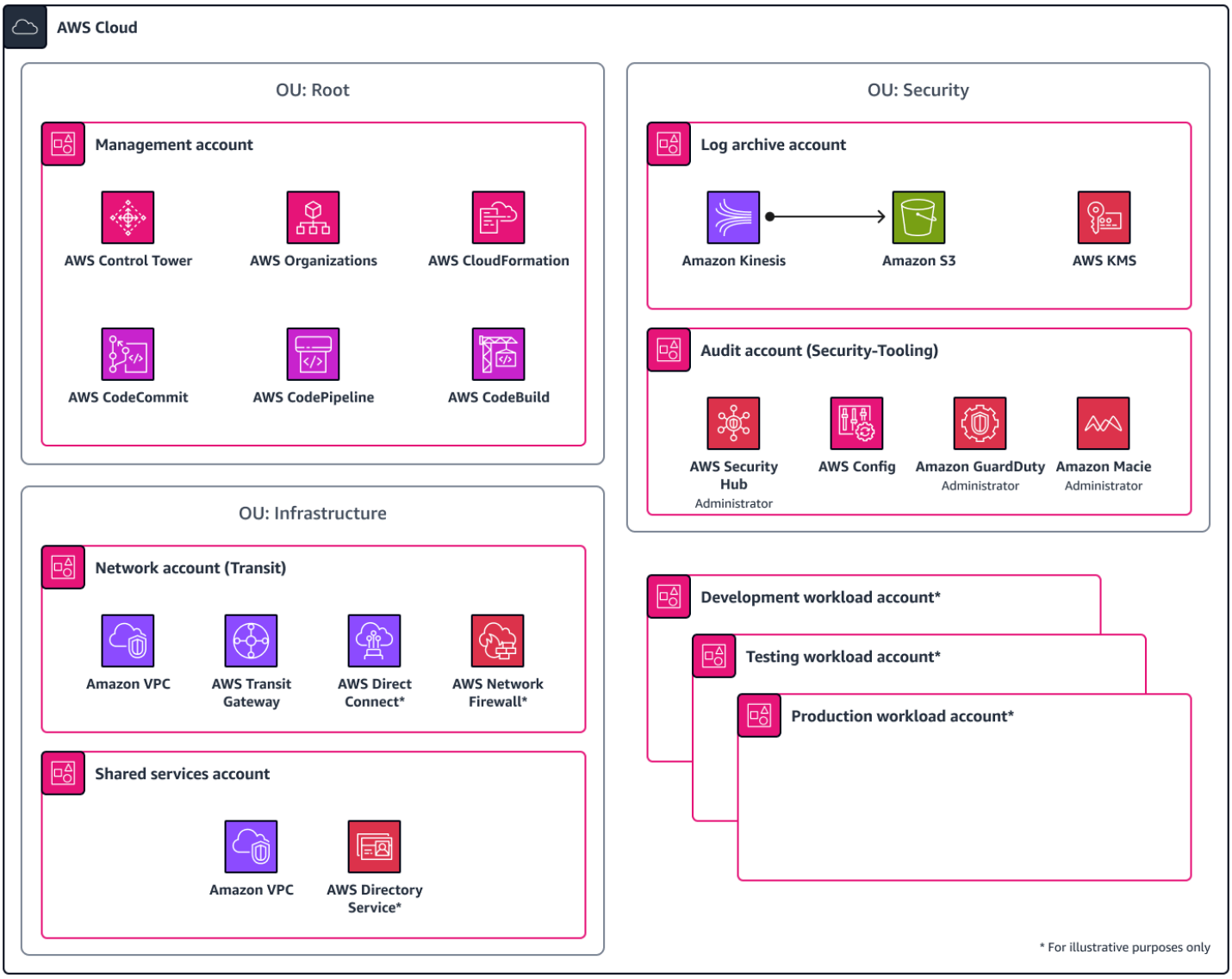
ID	VDMSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
	su host (HBSS), o un sistema equivalente approvato, per gestire la sicurezza degli endpoint per tutte le enclavi all'interno del. CSE			
2.1.3.3	VDMSForniranno servizi di identità che includeranno un risponditore Online Certificate Status Protocol (OCloudWorkload Security) per l'autenticazione a due fattori del sistema remoto DoD Common Access Card (CAC) degli utenti privilegiati del DoD su sistemi istanziati all'interno del. CSE	Autenticazione a più fattori () disponibile tramite: MFA AWS Identity and Access Management (IAM) AWS IAM Identity Center AWS Directory Service for Microsoft Active Directory AWS Private Certificate Authority	Configura una CAC carta per Amazon WorkSpaces	Parzialmente coperto

ID	VDMSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.3.4	VDMSDevono fornire un sistema di gestione della configurazione e degli aggiornamenti per servire sistemi e applicazioni per tutte le enclavi all'interno del. CSE	AWS Systems Manager Gestione patch AWS Config	Automatizzazione della gestione delle patch con AWS Systems Manager (video) YouTube	Parzialmente coperto
2.1.3.5	VDMSDevono fornire servizi di dominio logici che includano l'accesso alle directory, la federazione delle directory, il Dynamic Host Configuration Protocol (DHCP) e il Domain Name System (DNS) per tutte le enclavi all'interno di. CSE	AWS Managed Microsoft AD Amazon Cloud Privato Virtuale (AmazonVPC) Amazon Route 53	Configura DNS gli attributi per il tuo VPC	Parzialmente coperto

ID	VDMSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.3.6	VDMSDevono fornire una rete per la gestione dei sistemi e delle applicazioni all'interno dell'area CSE che sia logicamente separata dagli utenti e dalle reti di dati.	Amazon VPC VPCSottoreti Amazon	N/D	Coperto
2.1.3.7	VDMSFornirà un sistema di registrazione e archiviazione degli eventi di sistema, sicurezza, applicazione e attività degli utenti per la raccolta, l'archiviazione e l'accesso comuni ai registri degli eventi da parte degli utenti privilegiati che svolgono e svolgono attività. BCP MCP	AWS Security Hub AWS CloudTrail CloudWatch Registri Amazon Amazon Simple Storage Service (Amazon S3)	Registrazione centralizzata con OpenSearch	Coperto

ID	VDMSrequisito di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.3.8	VDMSDovranno provvedere allo scambio degli attributi di autenticazione e autorizzazione degli utenti privilegiati del DoD con il sistema di gestione delle identità e degli accessi CSP del DoD per consentire il provisioning, l'implementazione e la configurazione del sistema cloud.	AWS Managed Microsoft AD	Migliora la tua configurazione di sicurezza AWS Managed Microsoft AD	Non coperto
2.1.3.9	VDMSDevono implementare le capacità tecniche necessarie per svolgere la missione e gli obiettivi del ruolo. TCCM	AWS Managed Microsoft AD IAM IAMCentro di identità	N/D	Parzialmente coperto

Come mostrato nell'immagine seguente, LZA pone i componenti fondamentali per soddisfare i requisiti di VDMS base. Una volta implementato, LZA è necessario configurare alcuni componenti aggiuntivi per soddisfare gli standard. VDMS Nella tabella precedente, assicurati di esaminare i collegamenti nella colonna Risorse aggiuntive. Questi collegamenti consentono di configurare questi elementi aggiuntivi o forniscono ulteriori miglioramenti della sicurezza.



Integrazione di servizi supplementari

La colonna Risorse aggiuntive della tabella precedente elenca le risorse che consentono di ampliare la gamma di risorse necessarie LZA per soddisfare VDMS i requisiti. AWS offre inoltre alcuni materiali da workshop per aiutarti a configurare un'architettura cloud sicura. Senza modifiche, LZA soddisfa

i IL5 requisitiIL4/, ma puoi implementare servizi aggiuntivi per migliorare la sicurezza del tuo AWS ambiente.

Ad esempio, Amazon Inspector è un servizio di gestione delle vulnerabilità che analizza continuamente i AWS carichi di lavoro alla ricerca di vulnerabilità del software ed esposizione involontaria della rete. Puoi usarlo per identificare e analizzare le vulnerabilità nei sistemi operativi host, come Windows e Linux. Sebbene Amazon Inspector non includa completamente tutti i requisiti necessari per un sistema di sicurezza basato su host (HBSS), fornisce almeno una valutazione della vulnerabilità di livello base delle istanze.

Applicazione di patch del sistema operativo

L'applicazione di patch al sistema operativo è un componente fondamentale del funzionamento di un ambiente sicuro. AWS offre e consiglia l'utilizzo di Patch Manager, una funzionalità di AWS Systems Manager, per mantenere linee di base coerenti per le patch e automatizzare la distribuzione delle patch. Patch Manager automatizza il processo di applicazione di patch ai nodi gestiti sia con aggiornamenti relativi alla sicurezza che con altri tipi di aggiornamenti.

Gestione patch consente di applicare patch sia per i sistemi operativi sia per le applicazioni (In Windows Server, il supporto delle applicazioni è limitato agli aggiornamenti per le applicazioni rilasciate da Microsoft.) Per ulteriori informazioni, consulta Orchestrazione di processi di patch personalizzati in più fasi utilizzando Patch Manager sul AWS Systems Manager blog AWS Cloud Operations and Migrations.

Per step-by-step istruzioni sull'uso di Patch Manager, consultate il workshop sugli strumenti di AWS gestione e governance.

Per ulteriori informazioni sulla protezione dei carichi di lavoro Microsoft Windows su AWS, consulta il Workshop Proteggere i carichi di lavoro Windows. AWS

Cloud Credential Manager affidabile

Trusted Cloud Credential Manager (TCCM) è un componente di. SCCA È responsabile della gestione delle credenziali. Quando si stabilisce ilTCCM, è importante consentire l'accesso con il minimo privilegio a. SCCA Ciò può essere ottenuto utilizzando i servizi di gestione delle AWS identità e degli accessi. Un componente aggiuntivo di TCCM è una connessione al Virtual Data Center Managed Services (VDMS). È possibile utilizzare questa connessione secondo necessità per accedere AWS Management Console a e gestire ilTCCM.

TCCMÈ una combinazione di tecnologie e standard che regolano l'accesso a AWS. TCCMÈ considerato fondamentale per la maggior parte delle implementazioni perché controlla le autorizzazioni di accesso. La TCCM funzione non è destinata a imporre requisiti univoci di gestione delle identità al fornitore di servizi cloud commerciale ()CSP. TCCMInoltre, non vieta l'uso di soluzioni di federazione CSP DoD o di broker di identità di terze parti per fornire il controllo dell'identità previsto.

I componenti della TCCM politica si basano su una comprensione generale che CSPs offre un sistema di gestione delle identità e degli accessi che consente il controllo dell'accesso ai sistemi cloud. Tali sistemi possono includere la console CSP di accesso e i componenti API del servizio di interfaccia a riga di comando (CLI). A livello base, TCCM devono bloccare le credenziali che possono essere utilizzate per creare reti e altre risorse non autorizzate. TCCMÈ nominato dall'Autorizzatore (AO) incaricato della supervisione dei sistemi IT. Le TCCM politiche stabiliscono la necessità di un modello di accesso con privilegi minimi. Queste policy sono responsabili della fornitura e del controllo delle credenziali degli utenti privilegiati nel cloud commerciale. Questo per rimanere in linea con la Guida ai requisiti di sicurezza del cloud computing del DoD, che riguarda l'implementazione di politiche, piani e procedure per la gestione delle credenziali dell'account del portale. Prima della connessione al Defense Information Systems Network (DISN), DISA convalida l'esistenza del Cloud Credential Management Plan (CCMP) come parte del processo di approvazione della connessione definito nella Connection Process Guide.

La tabella seguente contiene i requisiti minimi per. TCCM Spiega se LZA soddisfa ogni requisito e quali possono essere utilizzati per Servizi AWS soddisfarli.

ID	TCCMrequisiti di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.4.1	TCCMDeve sviluppare e mantenere un piano di gestione delle credenziali cloud (CCMP) per affrontare l'implementazione di politiche, piani	N/D	N/D	Non coperto

ID	TCCMrequisiti di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
	e procedure che verranno applicati alla gestione delle credenziali degli account del titolare della missione nel portale clienti.			
2.1.4.2	TCCMRaccoglierà, controllerà e archivierà tutti i registri delle attività e gli avvisi del Customer Portal.	AWS CloudTrail CloudWatch Registri Amazon	N/D	Coperto
2.1.4.3	TCCMGarantiscono che gli avvisi del registro delle attività siano condivisi, inoltrati o recuperabili dagli utenti privilegiati del DoD coinvolti in attività e attività. MCP BCP	AWS CloudTrail CloudWatch Registri Servizio di notifica semplice Amazon (AmazonSNS) CloudWatch Approfondimenti sui registri	N/D	Coperto

ID	TCCMrequisiti di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.4.4	Se necessario per la condivisione delle informazioni, TCCM devono creare account di accesso agli archivi di registro per l'accesso ai dati del registro delle attività da parte degli utenti privilegiati che svolgono entrambe le attività. MCP BCP	AWS CloudTrail CloudWatch Registri Amazon SNS CloudWatch Approfondimenti sui registri	N/D	Coperto
2.1.4.5	TCCMDovrà recuperare e controllare in modo sicuro le credenziali dell'account del portale clienti prima della connettività dell'applicazione della missione al. DISN	AWS IAM Identity Center	N/D	Coperto

ID	TCCMrequisiti di sicurezza	AWS tecnologie	Risorse aggiuntive	Coperto da LZA
2.1.4.6	TCCMDeve creare, emettere e revocare, se necessario, le credenziali del portale clienti con accesso meno privilegiato in base ai ruoli agli amministratori dell'applicazione e del sistema del proprietario della missione (ad esempio, utenti con privilegi DoD).	AWS Identity and Access Management (IAM) AWS Directory Service for Microsoft Active Directory	N/D	Coperto

Per consentire di TCCM soddisfare i requisiti, LZA utilizza il controllo programmatico delle risorse tramite il IAM servizio. È inoltre possibile combinare IAM con AWS Managed Microsoft AD per implementare il Single Sign-On in un'altra directory. Questo collega AWS l'ambiente all'infrastruttura locale con trust di Active Directory. InLZA, l'implementazione viene implementata con IAM ruoli per l'accesso temporaneo basato sulla sessione, i IAM ruoli sono credenziali di breve durata che aiutano l'organizzazione a soddisfare i requisiti necessari. TCCM

Sebbene LZA implementi l'accesso con privilegi minimi e l'accesso programmatico a breve termine alle AWS risorse, esamina le IAMmigliori pratiche per assicurarti di seguire le linee guida di sicurezza consigliate.

Per ulteriori informazioni sull'implementazione AWS Managed Microsoft AD, consulta la AWS Managed Microsoft ADsezione del workshop Active Directory on AWS Immersion Day.

Il modello di responsabilitàAWS condivisa si applica a TCCM e alLZA. LZASviluppa gli aspetti fondamentali del controllo degli accessi, ma ogni organizzazione è responsabile della configurazione dei propri controlli di sicurezza.

Conclusioni e risorse

Per il Dipartimento della Difesa degli Stati Uniti (DoD), questa guida spiega quali sono i requisiti della Defense Information Systems Agency (DISA) per l'implementazione di un'architettura di cloud computing sicura (). SCCA Utilizzando Landing Zone Accelerator (LZA) on AWS, è possibile implementare AWS offerte ed eliminare il lavoro indifferenziato e faticoso. Questo ti aiuta a concentrarti sulla tua missione di creare un'infrastruttura cloud conforme o IL4 conforme. IL5

AWS risorse

- AWS Servizi rientranti nell'ambito del programma di AWS conformità (conformità)
- Guida ai requisiti di sicurezza del cloud computing del Dipartimento della Difesa (AWS conformità)
- AWS Guide alla conformità dei clienti (AWS conformità)
- Landing Zone Accelerator attivo AWS (Libreria di AWS soluzioni)
- Guida all'implementazione di Landing Zone Accelerator on AWS
- SCCAsul diagramma AWS GovCloud dell'architettura
- Infrastruttura cloud come codice (IaC) del Dipartimento della Difesa per AWS()Marketplace AWS

Altre risorse

- Guida ai requisiti di sicurezza del cloud computing (DISAsito web)
- Progetto di riferimento del punto di accesso nativo del cloud (DoD) del Dipartimento della Difesa (DoDCNAP) (sito Web del DoD)
- Scheda informativa sull'architettura DoD Secure Cloud Computing (sito web) DISA
- DODCloud IAc (hosting ed elaborazione J9)

Cronologia dei documenti

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

Modifica	Descrizione	Data
Pubblicazione iniziale	—	12 marzo 2024

AWS Glossario delle linee guida prescrittive

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

Numeri

7 R

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

- Rifattorizzare/riprogettare: trasferisci un'applicazione e modifica la sua architettura sfruttando appieno le funzionalità native del cloud per migliorare l'agilità, le prestazioni e la scalabilità. Ciò comporta in genere la portabilità del sistema operativo e del database. Esempio: migra il tuo database Oracle locale all'edizione compatibile con Amazon Aurora SQL Postgre.
- 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 (AmazonRDS) 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: migrare un Microsoft Hyper-V applicazione a. 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.

ACID

Scopri atomicità, coerenza, isolamento e 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 SQL funzione 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 utilizzata nella strategia di AWS migrazione, consulta la guida all'integrazione delle operazioni.

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durata () 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 sugli attributi () ABAC

La pratica di creare autorizzazioni dettagliate basate su attributi utente, come reparto, ruolo professionale e nome del team. Per ulteriori informazioni, vedere ABACfor 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 Framework di adozione del cloud ()AWS CAF

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 CAForganizza 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 del personale, la formazione e le comunicazioni per aiutare l'organizzazione a un'adozione efficace del cloud. Per ulteriori informazioni, consulta il AWS CAFsito Web e il AWS CAFwhite paper.

AWS Quadro di qualificazione del carico di lavoro ()AWS WQF

Uno strumento che valuta i carichi di lavoro di migrazione dei database, consiglia strategie di migrazione e fornisce stime del lavoro. AWS WQFè 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 falliti, API chiamate 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.

modifica l'acquisizione dei dati (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 utilizzarlo CDC per vari scopi, come 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 i CCoEpost 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 zoneCCoE, 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 comuni includono GitHub oppure Bitbucket Cloud. Ogni versione del codice è denominata branch.

In una struttura a microservizi, ogni repository è dedicato a una singola funzionalità. Una singola pipeline CI/CD può utilizzare più repository.

cache fredda

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

dati freddi

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

visione artificiale (CV)

Un campo dell'intelligenza artificiale che utilizza l'apprendimento automatico per analizzare ed estrarre informazioni da formati visivi come immagini e video digitali. Ad esempio, AWS Panorama offre dispositivi che aggiungono CV alle reti di telecamere locali e Amazon SageMaker fornisce algoritmi di elaborazione delle immagini per CV.

deriva della configurazione

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

database CMDB di gestione della configurazione ()

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 provenienti da una CMDB fase di individuazione e analisi del portafoglio durante la migrazione.

Pacchetto di conformità

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

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

Il processo di automazione delle fasi di origine, creazione, test, gestione temporanea e produzione del processo di rilascio del software. CI/CD is commonly described as a pipeline. CI/CDpuò

aiutarti 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 di 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. DVSMestende 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 lo strangler fig pattern, vedi Modernizing legacy Microsoft. ASP NET(ASMX) servizi web in modo incrementale utilizzando contenitori e Amazon API Gateway.

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.

EDI

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 commerciali 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) per condividerlo con altri utenti. È possibile 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 responsabili possono connettersi al servizio endpoint in modo privato creando endpoint di interfaccia. VPC Per ulteriori informazioni, consulta Creare un servizio endpoint nella documentazione di Amazon Virtual Private Cloud (AmazonVPC).

pianificazione delle risorse aziendali () ERP

Un sistema che automatizza e gestisce i processi aziendali chiave (come la contabilità e MESla 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 relative AWS CAF alla sicurezza includono la gestione delle identità e degli accessi, i controlli investigativi, la sicurezza dell'infrastruttura, la protezione dei dati e la risposta agli incidenti. Per ulteriori informazioni sulle epiche, consulta la strategia di migrazione AWS , consulta la guida all'implementazione del programma.

ERP

Vedi la pianificazione delle risorse aziendali.

analisi esplorativa dei dati () EDA

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

F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

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

prompt con pochi scatti

Fornire un LLMnumero 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 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. FMssono 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 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 implementate utilizzando le politiche di controllo del servizio e i limiti delle IAM autorizzazioni. 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 blocco

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

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

I

IaC

Vedi l'infrastruttura come codice.

Policy basata su identità

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

applicazione inattiva

Un'applicazione con un utilizzo medio CPU e della memoria 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.

in entrata (ingresso) VPC

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

migrazione incrementale

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

Internet delle cose industriale () IIoT

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

ispezione VPC

In un'architettura AWS multi-account, un'architettura centralizzata VPC 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 funzioni 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. ITILfornisce le basi perITSM.

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 ITSM gli strumenti, 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 dell'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. An LLM può eseguire 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.

LBAC

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 Applicare le autorizzazioni con privilegi minimi nella documentazione. 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.

MES

Vedi Manufacturing Execution System.

Trasporto di telemetria in accodamento dei messaggi () 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 MAP di accelerazione della migrazione ()

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

migrazione su larga scala

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

fabbrica di migrazione

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portafoglio di migrazione () MPA

Uno strumento online che fornisce informazioni per la convalida del business case per la migrazione a. Cloud AWS MPAfornisce una valutazione dettagliata del portafoglio (dimensionamento corretto dei server, prezzi, TCO confronti, 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 MPAstrumento (richiede l'accesso) è disponibile gratuitamente per tutti i consulenti e i consulenti partner. AWS 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. AWS CAF Per ulteriori informazioni, consulta la guida di preparazione alla migrazione. MRAè 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.

MPA

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.

OAI

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 accordi tra i gruppi IT funzionali si impegnano a fornire i risultati reciproci, a supporto di un accordo sui livelli 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 AWS Well-Architected 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 delle modifiche organizzative (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. OCMaiuta le organizzazioni a prepararsi e a passare a nuovi sistemi e strategie accelerando l'adozione del cambiamento, affrontando le questioni transitorie 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, consulta la OCMguida.

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). OACsupporta tutti i bucket S3 in generale Regioni AWS,

la crittografia lato server con AWS KMS (SSE-KMS) e la crittografia dinamica `PUT` e `DELETE` le richieste al bucket S3.

identità OAI di accesso all'origine ()

In CloudFront, un'opzione per limitare l'accesso per proteggere i tuoi contenuti Amazon S3. Quando lo usiOAI, 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 offre un controllo degli accessi più granulare e avanzato.

ORR

Vedi la revisione della prontezza operativa.

- NON

Vedi la tecnologia operativa.

in uscita (uscita) VPC

In un'architettura AWS multi-account, 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 politica di IAM gestione associata ai IAM principali per impostare le autorizzazioni massime che l'utente o il ruolo possono avere. Per ulteriori informazioni, consulta Limiti delle autorizzazioni nella documentazione. 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. Alcuni esempi PII includono nomi, indirizzi e informazioni di contatto.

PII

Visualizza 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`true`. `false` `WHERE`

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, un IAM ruolo o un utente. Per ulteriori informazioni, consulta i termini e i concetti di Principal in Roles nella IAM documentazione.

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 DNS richieste relative a un dominio e ai 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 LLMprompt come input per il prompt successivo per generare risposte migliori. Questa tecnica viene utilizzata per suddividere un'attività complessa in sottoattività o per rifinire 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 sistema basato su microservizi MES, 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 SQL relazionale.

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

RACImatrice

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

RAG

Vedi Retrieval Augmented Generation.

ransomware

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

RASCImatrice

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 utilizzare Regioni AWS il proprio 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 responsabile, responsabile, consultata, informata () 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 RASCImatrice e se la escludi, viene chiamata RACImatrice.

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.

Generazione aumentata di recupero () RAG

Una tecnologia di intelligenza artificiale generativa in cui un LLMfa riferimento a una fonte di dati autorevole esterna alle sue fonti di dati di addestramento prima di generare una risposta. Ad esempio, un RAG modello potrebbe eseguire una ricerca semantica nella knowledge base o nei dati personalizzati di un'organizzazione. Per ulteriori informazioni, consulta Cos'è 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 SQL espressioni di base e flessibili con regole di accesso definite. RCACè costituito da permessi di riga e maschere di colonna.

RPO

Vedi 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

SAML2.0

Uno standard aperto utilizzato da molti provider di identità (IdPs). Questa funzionalità abilita il single sign-on federato (SSO), in modo che gli utenti possano accedere AWS Management Console o richiamare le AWS API operazioni senza che sia necessario creare un account utente IAM per tutti i membri dell'organizzazione. Per ulteriori informazioni sulla federazione SAML basata sulla versione 2.0, vedere Informazioni sulla federazione basata sulla versione SAML 2.0 nella documentazione. 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 di gestione degli eventi di sicurezza (SEM). Un SIEM sistema 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 di 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 VPC sicurezza, l'applicazione di patch a un'EC2istanza Amazon o la rotazione delle credenziali.

Crittografia lato server

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

politica di controllo del servizio (SCP)

Una policy che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in AWS Organizations. SCPsdefinisci barriere o imposta 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

Il punto URL 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.

singolo punto di errore (SPOF)

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

SLA

Vedi il contratto sui livelli di servizio.

SLI

Vedi l'indicatore del livello di servizio.

SLO

Vedi l'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

Vedere Single Point of Failure.

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, vedi Modernizing legacy MicrosoftASP. NET(ASMX) servizi web in modo incrementale utilizzando contenitori e Amazon API Gateway.

sottorete

Una gamma di indirizzi IP nel tuoVPC. 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

Tecnica per fornire contesto, istruzioni o linee guida a un utente per LLMindirizzarne il comportamento. I prompt di sistema aiutano a definire 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.

VPCscrutando

Una connessione tra due VPCs che consente di indirizzare il traffico utilizzando indirizzi IP privati. Per ulteriori informazioni, consulta What is VPC peering nella VPC documentazione di Amazon.

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 SQL funzione 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.

WORM

Vedi write once, read many.

WQF

Vedi AWSWorkload Qualification Framework.

scrivi una volta, leggi molte () WORM

Un modello di archiviazione 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

Fornisce istruzioni per eseguire un'LLMattività, ma non fornisce esempi (immagini) che possano aiutarla. LLMDeve utilizzare le proprie 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 con un utilizzo medio CPU e della 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.