Adottare Zero Trust: una strategia per una trasformazione aziendale agile e sicura

AWS Guida prescrittiva

AWS Guida prescrittiva: Adottare Zero Trust: una strategia per una trasformazione aziendale agile e sicura

Table of Contents

Adottare Zero Trust: una strategia per una trasformazione aziendale agile e sicura

Greg Gooden, Amazon Web Services (AWS)

Dicembre 2023 (cronologia dei documenti)

Oggi più che mai, la sicurezza rappresenta una priorità essenziale per le organizzazioni. Dare importanza alla sicurezza comporta una serie di benefici, tra cui la salvaguardia della fiducia dei clienti, il potenziamento della mobilità del personale e la creazione di nuove opportunità nel settore del business digitale. Nel gestire la sicurezza, le aziende si trovano di fronte a un classico interrogativo: quali sono le strategie migliori per assicurare adeguati livelli di sicurezza e disponibilità per i dati e i sistemi? Zero Trust è il termine oramai più diffuso per descrivere la risposta moderna a questa domanda.

L'architettura Zero Trust (ZTA) è un modello concettuale e l'insieme dei meccanismi associati che si concentrano sull'offerta di controlli di sicurezza delle risorse digitali che non dipendono in modo esclusivo o fondamentale dai controlli di rete o dai perimetri di rete tradizionali. Al contrario, i controlli di rete incorporano elementi relativi alle identità, ai dispositivi, ai comportamenti e ad altri segnali e aspetti contestuali per prendere decisioni di accesso più granulari, intelligenti e adattive su base continuativa. Implementando un modello ZTA, è possibile compiere un passo significativo nel percorso incessante di maturazione della sicurezza informatica e dei concetti di difesa in profondità in particolare.

Processi decisionali

L'implementazione di una strategia ZTA richiede un'attenta pianificazione e un processo decisionale accurato. Implica la valutazione di vari fattori e il loro allineamento agli obiettivi dell'organizzazione. I processi decisionali essenziali per intraprendere un percorso ZTA includono:

1. Coinvolgimento delle parti interessate: è fondamentale coinvolgere altri CxOs dirigenti e senior manager per comprendere le loro priorità, preoccupazioni e visione per la posizione di sicurezza dell'organizzazione. VPs Coinvolgendo le principali parti interessate sin dalle fasi iniziali, è possibile allineare l'implementazione della ZTA agli obiettivi strategici generali e ottenere il supporto e le risorse necessari.

2. Valutazione del rischio: condurre una valutazione completa del rischio permette di identificare i problemi, la superficie eccessiva e le risorse critiche, il che aiuta a prendere decisioni informate sugli investimenti e sui controlli di sicurezza. Valuta l'assetto di sicurezza attuale della tua organizzazione, identifica i potenziali punti deboli e dai priorità alle aree di miglioramento in base al panorama di rischio specifico del settore e dell'ambiente operativo.
3. Valutazione della tecnologia: la valutazione dell'attuale panorama tecnologico dell'organizzazione e l'identificazione delle lacune contribuiscono alla selezione di strumenti e soluzioni appropriati in linea con i principi ZTA. Questa valutazione dovrebbe includere un'analisi approfondita dei seguenti aspetti:
   - Architettura di rete
   - Sistemi di gestione dell'identità e degli accessi
   - Meccanismi di autenticazione e autorizzazione
   - Gestione unificata degli endpoint
   - Strumenti e processi di proprietà delle risorse
   - Tecnologie di crittografia
   - Funzionalità di monitoraggio e registrazione
   - La scelta dello stack tecnologico giusto è fondamentale per creare un modello ZTA solido.
4. Gestione del cambiamento: è essenziale riconoscere gli impatti culturali e organizzativi dell'adozione di un modello ZTA. L'implementazione di pratiche di gestione del cambiamento contribuisce a garantire la fluidità della transizione e dell'accettazione in tutta l'organizzazione. Implica la formazione dei dipendenti sui principi e sui vantaggi della ZTA così come sulle nuove pratiche di sicurezza, nonché la promozione di una cultura attenta alla sicurezza che incoraggi la responsabilità e l'apprendimento continuo.

Questa guida prescrittiva mira a fornire CxOs, e ai dirigenti senior VPs, una strategia completa per l'implementazione di ZTA. Approfondirà gli aspetti chiave della ZTA, tra cui:

- Preparazione dell'organizzazione
- Approcci di adozione graduale
- Collaborazione delle parti interessate
- Best practice per realizzare una trasformazione aziendale agile e sicura

Seguendo queste linee guida, la tua organizzazione può navigare nel panorama ZTA e ottenere risultati di successo nel tuo percorso di sicurezza nel cloud Amazon Web Services (AWS). AWS offre una varietà di servizi che puoi utilizzare per implementare uno ZTA, come AWS Identity and Access Management (IAM) Accesso verificato da AWS, Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway e Amazon. GuardDuty Questi servizi possono aiutare a proteggere le risorse da accessi non autorizzati AWS .

Obiettivi aziendali specifici

Questa sezione illustra i risultati attesi associati alla definizione e all'implementazione di un'architettura Zero Trust nell'organizzazione.

Assetto di sicurezza migliorato

Adottando i principi di Zero Trust, l'organizzazione può rafforzare il proprio assetto di sicurezza, mitigare i rischi per la sicurezza e proteggere l'infrastruttura e i dati cloud. Il principio fondamentale di Zero Trust di concedere l'accesso su need-to-know base regolare, abbinato a controlli rigorosi, riduce significativamente la superficie e limita il potenziale impatto degli eventi di sicurezza. Questo approccio proattivo aiuta le organizzazioni a stare al passo con i rischi di sicurezza emergenti e contribuisce a garantire la riservatezza, l'integrità e la disponibilità delle risorse.

Adozione del cloud senza intoppi

Lo sviluppo di un piano di adozione dell'architettura Zero Trust (ZTA) ben definito può contribuire a garantire una transizione fluida e di successo verso l'ambiente cloud. I principi della ZTA sono strettamente allineati alle best practice di sicurezza del cloud, fornendo alle organizzazioni una base e sicura dalla quale beneficiare dei vantaggi del cloud computing. L'integrazione dei principi della ZTA sin dalle fasi iniziali aiuta l'organizzazione a progettare la propria architettura cloud incentrandola sulla sicurezza.

Conformità e allineamento normativo

L'implementazione delle pratiche della ZTA può aiutare l'organizzazione a soddisfare i requisiti e gli standard normativi e di settore. ZTA promuove intrinsecamente il principio del privilegio minimo e impone controlli degli accessi rigorosi. I controlli degli accessi sono spesso imposti da normative quali le seguenti:

- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS).

Adottando Zero Trust, l'organizzazione può contribuire a dimostrare il proprio impegno nei confronti della protezione dei dati, della privacy e della conformità normativa, riducendo al minimo il rischio di sanzioni o danni alla reputazione.

Migliore protezione dei dati

Le organizzazioni possono proteggere i dati sensibili durante tutto il processo di adozione del cloud implementando la crittografia dei dati, i controlli degli accessi e le valutazioni periodiche della sicurezza. L'organizzazione può adottare le seguenti iniziative specifiche:

- Crittografia dei dati: la crittografia dei dati è il processo che trasforma i dati in chiaro in testo cifrato; per eseguire l'operazione inversa, ossia decrittografare i dati nel formato di testo non crittografato originale, è necessaria una chiave. Ciò rende molto più difficile per le persone non autorizzate accedere ai dati sensibili, anche se sono in grado di ottenere una copia dei dati.
- Controlli degli accessi: i controlli degli accessi limitano chi può accedere ai dati sensibili e le operazioni che può eseguire con essi. A tale scopo è possibile assegnare ruoli e autorizzazioni agli utenti e utilizzare l'autenticazione a più fattori o altri metodi per verificare l'identità dell'utente.
- Valutazioni periodiche della sicurezza: le valutazioni periodiche della sicurezza possono aiutare le organizzazioni a identificare e risolvere i problemi di sicurezza e risolverli in modo proattivo. Queste valutazioni possono essere condotte da team di sicurezza interni o da società di sicurezza esterne.

Le architetture Zero Trust adottano un approccio globale alla protezione dei dati implementando una serie di misure di sicurezza. Queste misure includono l'autenticazione avanzata, la crittografia dei dati e i controlli granulari degli accessi. Questo approccio riduce al minimo il rischio di eventi di sicurezza relativi ai dati e protegge le informazioni sensibili dagli accessi non autorizzati.

Risposta agli incidenti efficace

Le organizzazioni possono rilevare e rispondere agli eventi di sicurezza in modo più rapido ed efficace stabilendo framework di monitoraggio e risposta agli incidenti nell'ambiente cloud. Le architetture Zero Trust enfatizzano il monitoraggio continuo, l'integrazione dell'intelligence sulle minacce e la visibilità in tempo reale delle attività degli utenti, del traffico di rete e del comportamento del sistema. I team di sicurezza possono quindi identificare e mitigare in modo proattivo gli eventi di sicurezza. Questo approccio riduce il tempo necessario per rilevare e rispondere a potenziali problemi e minimizza l'impatto sulle operazioni aziendali. I punti chiave includono i seguenti:

- Test: indipendentemente dal framework o dalla metodologia di risposta agli incidenti scelta dall'organizzazione, è necessario testare regolarmente il piano di risposta agli incidenti. Gli esercizi da scrivania, le simulazioni e il red teaming offrono l'opportunità di mettere in pratica la risposta agli incidenti in ambienti realistici, scoprire le lacune in termini di strumenti e capacità, e sviluppare l'esperienza e la sicurezza degli addetti alle operazioni di risposta agli incidenti.
- Monitoraggio: è necessario monitorare continuamente gli ambienti cloud per rilevare eventuali segni di attività anomale. Per farlo, è possibile avvalersi di una varietà di strumenti e tecniche, come l'analisi dei log, il monitoraggio della rete e la scansione delle vulnerabilità.
- Integrazione dell'intelligence sulle minacce: l'intelligence sulle minacce va integrata nei framework di monitoraggio e risposta agli incidenti. Questo aiuta l'organizzazione a identificare e rispondere alle minacce in modo più rapido ed efficace.
- Visibilità in tempo reale: per identificare e rispondere rapidamente agli incidenti di sicurezza, l'organizzazione ha bisogno di una visibilità in tempo reale sulle attività degli utenti, sul traffico di rete e sul comportamento del sistema.
- Identificazione e mitigazione proattive: identificando e mitigando in modo proattivo gli eventi di sicurezza, l'organizzazione può ridurre il tempo necessario per rilevare e rispondere alle potenziali minacce, riducendo al minimo l'impatto sulle operazioni aziendali.

Incremento della produttività della forza lavoro

Alla forza lavoro moderna occorre flessibilità per svolgere le proprie mansioni da una gamma sempre maggiore di luoghi e dispositivi e in ogni fascia oraria. Implementando la ZTA, è possibile supportare questi requisiti e migliorare la mobilità, la produttività e la soddisfazione della forza lavoro, mantenendo o migliorando al contempo l'assetto di sicurezza dell'organizzazione.

Abilitazione della trasformazione digitale

Sempre più spesso le organizzazioni perseguono l'interconnessione di dispositivi, macchine, strutture, infrastrutture e processi al di fuori del perimetro di rete tradizionale come parte della trasformazione digitale. I dispositivi Internet of Things (IoT) e tecnologia operativa (OT, nota anche come Industrial Internet of Things o IIo T) spesso trasmettono informazioni di telemetria e manutenzione predittiva direttamente al cloud. Per proteggere i carichi di lavoro, ciò richiede l'applicazione di controlli di sicurezza che vadano oltre il tradizionale approccio perimetrale.

Riepilogo della sezione

Concentrandosi su questi obiettivi stabiliti, l'organizzazione può sfruttare appieno il potenziale di ZTA e rafforzare il proprio assetto di sicurezza nel cloud. È importante allineare questi risultati con gli obiettivi specifici dell'organizzazione, adattarli ai requisiti specifici dell'azienda e valutarne regolarmente l'efficacia per promuovere il miglioramento continuo.

Comprensione dei principi di Zero Trust

L'architettura Zero Trust (ZTA) si basa su una serie di principi fondamentali che costituiscono la base del suo modello di sicurezza. La comprensione di questi principi è essenziale per le organizzazioni che desiderano adottare una strategia ZTA in modo efficace. Questa sezione tratta i principi fondamentali della ZTA.

Verifica e autenticazione

Il principio di verifica e autenticazione sottolinea l'importanza della solidità dell'identificazione e dell'autenticazione per i principali di tutti i tipi, inclusi utenti, macchine e dispositivi. La ZTA richiede una verifica continua delle identità e dello stato di autenticazione durante una sessione, idealmente ad ogni richiesta. Non si limita a fare affidamento unicamente sulla posizione della rete o sui tradizionali controlli ad essa associati. Questo approccio comporta l'adozione di un'autenticazione a più fattori (MFA) moderna e affidabile, e l'analisi di segnali aggiuntivi di natura ambientale e contestuale durante i processi di autenticazione. Adottando questo principio, le organizzazioni possono contribuire a garantire che le decisioni di autorizzazione in merito alle risorse possano beneficiare dei migliori input disponibili in termini di identità.

Accesso con privilegio minimo

Il principio del privilegio minimo prevede la concessione ai principali del livello minimo di accesso richiesto per svolgere i loro compiti. Adottando il principio dell'accesso con privilegio minimo, le organizzazioni possono applicare controlli granulari degli accessi, in modo che i principali abbiano accesso soltanto alle risorse necessarie per adempiere ai propri ruoli e responsabilità. Ciò include just-in-time l'implementazione del provisioning degli accessi, dei controlli degli accessi basati sui ruoli (RBAC) e delle revisioni periodiche degli accessi per ridurre al minimo la superficie e il rischio di accessi non autorizzati.

Microsegmentazione

La microsegmentazione è una strategia di sicurezza della rete che divide una rete in segmenti più piccoli e isolati per autorizzare flussi di traffico specifici. È possibile eseguire la microsegmentazione creando limiti per il carico di lavoro e applicando controlli di accesso rigorosi tra i diversi segmenti.

La microsegmentazione può essere implementata tramite la virtualizzazione della rete, il software-defined networking (SDN), firewall basati su host, elenchi di controllo degli accessi alla rete () e AWS funzionalità specifiche come i NACLs gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon) o. EC2 AWS PrivateLink I gateway di segmentazione controllano il traffico tra i segmenti per autorizzare esplicitamente l'accesso. I gateway di microsegmentazione e segmentazione aiutano le organizzazioni a limitare i percorsi superflui attraverso la rete, in particolare quelli che conducono a sistemi e dati critici.

Monitoraggio e analisi continui

Il monitoraggio e l'analisi continui implicano la raccolta, l'analisi e la correlazione di eventi e dati relativi alla sicurezza nell'ambiente dell'organizzazione. Implementando strumenti di monitoraggio e analisi affidabili, l'organizzazione è in grado di valutare i dati di sicurezza e la telemetria in modo convergente.

Questo principio sottolinea l'importanza della visibilità sul comportamento degli utenti, sul traffico di rete e sulle attività di sistema per identificare anomalie e potenziali eventi di sicurezza. Le tecnologie avanzate come la gestione delle informazioni e degli eventi di sicurezza (SIEM), l'analisi del comportamento degli utenti e delle entità (UEBA) e le piattaforme di intelligence sulle minacce svolgono un ruolo fondamentale nel conseguimento del monitoraggio continuo e del rilevamento proattivo delle minacce.

Automazione e orchestrazione

L'automazione e l'orchestrazione aiutano le organizzazioni a semplificare i processi di sicurezza, ridurre gli interventi manuali e migliorare i tempi di risposta. Automatizzando le attività di sicurezza di routine e utilizzando le funzionalità di orchestrazione, l'organizzazione può applicare policy di sicurezza coerenti e rispondere rapidamente agli eventi di sicurezza. Questo principio include anche l'automazione dei processi di fornitura e disattivazione degli accessi per garantire una gestione tempestiva e accurata delle autorizzazioni degli utenti. Adottando l'automazione e l'orchestrazione, l'organizzazione può migliorare l'efficienza operativa, ridurre gli errori umani e concentrare le risorse su iniziative di sicurezza più strategiche.

Autorizzazione

In una ZTA, ogni richiesta di accesso a una risorsa deve essere esplicitamente autorizzata da un punto di applicazione. Oltre all'identità autenticata, le policy di autorizzazione dovrebbero prendere

in considerazione altre informazioni contestuali, come l'integrità e l'assetto del dispositivo, i modelli di comportamento, la classificazione delle risorse e i fattori di rete. Il processo di autorizzazione dovrebbe prendere in considerazione questo contesto convergente in relazione alle policy di accesso pertinenti alla risorsa richiesta. Un contributo significativo può venire dai modelli di machine learning, capaci di integrare dinamicamente le policy dichiarative. Se utilizzati, questi modelli dovrebbero concentrarsi solo sulle restrizioni aggiuntive e non dovrebbero concedere un accesso che non sia stato esplicitamente specificato.

Riepilogo della sezione

Aderendo a questi principi fondamentali della ZTA, le organizzazioni possono stabilire un solido modello di sicurezza in linea con il carattere variegato del moderno ambiente aziendale. L'implementazione di questi principi richiede un approccio globale che combini tecnologia, processi e persone per raggiungere una mentalità Zero Trust e creare un assetto di sicurezza resiliente.

Componenti chiave di un'architettura Zero Trust

Per implementare efficacemente una strategia Zero Trust Architecture (ZTA), l'organizzazione deve comprendere i componenti costitutivi essenziali di una ZTA. Questi componenti si integrano per migliorare continuamente un modello di sicurezza completo che si allinea ai principi di Zero Trust. Questa sezione tratta i componenti essenziali della ZTA.

Gestione dell'identità e degli accessi

La gestione delle identità e degli accessi costituisce la base di una ZTA in quanto fornisce una solida autenticazione degli utenti e meccanismi granulari di controllo degli accessi. Include tecnologie come l'autenticazione unica (SSO), l'autenticazione a più fattori (MFA) e soluzioni di governance e gestione delle identità. La gestione delle identità e degli accessi offre un elevato livello di garanzia dell'autenticazione e un contesto importante che sono fondamentali per prendere decisioni di autorizzazione Zero Trust. Allo stesso tempo, la ZTA è un modello di sicurezza in cui l'accesso alle applicazioni e alle risorse viene concesso per ogni singolo utente, dispositivo e sessione. Questo aiuta a proteggere le organizzazioni dagli accessi non autorizzati anche nel caso in cui le credenziali di un utente siano compromesse.

Secure Access Service Edge

Secure Access Service Edge (SASE) è un nuovo approccio alla sicurezza di rete che virtualizza, combina e distribuisce le funzioni di rete e di sicurezza in un unico servizio basato sul cloud. SASE può fornire un accesso sicuro alle applicazioni e alle risorse a prescindere dalla posizione dell'utente.

SASE include una varietà di funzionalità di sicurezza, come gateway web sicuri, firewall as a service e accesso alla rete Zero Trust (ZTNA). Queste funzionalità interagiscono per proteggere le organizzazioni da un'ampia gamma di minacce, tra cui malware, phishing e ransomware.

Prevenzione della perdita di dati

Le tecnologie di prevenzione della perdita dei dati (DLP) possono aiutare le organizzazioni a proteggere i dati sensibili dalla divulgazione non autorizzata. Le soluzioni DLP monitorano e controllano i dati in transito e a riposo. Questo aiuta le organizzazioni a definire e applicare policy che impediscano gli eventi di sicurezza relativi ai dati, contribuendo a garantire che le informazioni sensibili rimangano protette in tutta la rete.

Gestione delle informazioni e degli eventi di sicurezza

Le soluzioni di gestione delle informazioni e degli eventi di sicurezza (SIEM) raccolgono, aggregano e analizzano i registri log eventi di sicurezza da varie origini all'interno dell'infrastruttura di un'organizzazione. Questi dati possono essere utilizzati per rilevare incidenti di sicurezza, facilitare la risposta agli incidenti e fornire informazioni su potenziali minacce e vulnerabilità.

Per la ZTA, in particolare, la capacità di una soluzione SIEM di correlare e comprendere la rispettiva telemetria proveniente da diversi sistemi di sicurezza è fondamentale per migliorare il rilevamento e la risposta ai modelli anomali.

Catalogo della proprietà delle risorse aziendali

Per concedere correttamente l'accesso alle risorse aziendali, un'organizzazione deve disporre di un sistema affidabile che cataloghi tali risorse e, soprattutto, chi le possiede. Questa fonte di verità deve fornire flussi di lavoro che facilitino le richieste di accesso, le relative decisioni di approvazione e le rispettive attestazioni periodiche. Col tempo, questa fonte di verità conterrà le risposte alla domanda "chi può accedere a cosa?" all'interno dell'organizzazione. Le risposte possono essere utilizzate sia per l'autorizzazione sia per il controllo e la conformità.

Gestione unificata degli endpoint

Oltre ad autenticare fortemente l'utente, una ZTA deve anche considerare l'integrità, l'assetto e lo stato del dispositivo dell'utente per valutare se l'accesso ai dati e alle risorse aziendali è sicuro. Una piattaforma di gestione unificata degli endpoint (UEM) offre le seguenti funzionalità:

- Provisioning dei dispositivi
- Configurazione e gestione delle patch continue
- Creazione di baseline di sicurezza
- Creazione di report di telemetria
- Pulizia e ritiro dei dispositivi

Punti di applicazione basati su policy

In una ZTA, l'accesso a ogni risorsa dovrebbe essere esplicitamente autorizzato da un punto di applicazione basato su policy. Inizialmente, questi punti di applicazione possono essere basati

sui punti di applicazione già esistenti nei sistemi di rete e di identità in uso. I punti di applicazione possono essere resi sempre più capaci alla luce della più ampia gamma di contesti e segnali forniti dalla ZTA. Nel lungo termine, l'organizzazione dovrebbe implementare punti di applicazione specifici per la ZTA che siano in grado di operare in un contesto convergente, integrare in modo coerente i fornitori di segnali, mantenere un set di policy completo e migliorare grazie alle informazioni raccolte dalla telemetria combinata.

Riepilogo della sezione

Per le organizzazioni che intendono adottare una ZTA è essenziale comprendere questi componenti chiave. Implementandoli e integrandoli in un modello di sicurezza coeso, l'organizzazione può stabilire un solido assetto di sicurezza basato sui principi di Zero Trust. Le sezioni seguenti esaminano la preparazione dell'organizzazione, gli approcci di adozione graduale e le best practice che contribuiscono a implementare con successo una ZTA all'interno dell'organizzazione.

Valutazione della preparazione dell'organizzazione all'adozione di Zero Trust

L'adozione di una nuova strategia di architettura è un impegno importante che richiede un'attenta pianificazione e un esame accurato dei fattori organizzativi. Questa sezione si concentra sulle considerazioni principali in merito alla preparazione dell'organizzazione all'adozione di Zero Trust in tutta l'azienda. Tenendo conto di queste considerazioni, l'organizzazione può porre le basi per un assetto di sicurezza più solido ed efficiente.

Allineamento della leadership e comunicazione con l'organizzazione

L'allineamento della leadership e la comunicazione con l'organizzazione sono essenziali per il successo dell'implementazione di Zero Trust. La leadership deve comprendere i vantaggi di Zero Trust e le risorse necessarie. Inoltre, i leader devono essere disposti ad apportare modifiche alla cultura e ai processi dell'organizzazione. La comunicazione con i dipendenti è necessaria per creare fiducia e consenso. I dipendenti devono comprendere il motivo per cui l'organizzazione implementa Zero Trust, le implicazioni per il proprio ruolo e il contributo che possono offrire. La comunicazione deve essere aperta, trasparente e continua.

Supporto e consenso della leadership

Per un'implementazione efficace di un'architettura Zero Trust (ZTA), è fondamentale allineare le principali parti interessate e i dirigenti sugli obiettivi, i vantaggi e le misure di successo dell'architettura. Condividi l'importanza dei principi di Zero Trust per migliorare la sicurezza e favorire l'agilità aziendale passando dalla tradizionale sicurezza basata sul perimetro a un approccio più granulare e incentrato sull'utente. Con questo nuovo approccio, l'organizzazione può adattarsi più rapidamente ai cambiamenti e alle minacce. L'allineamento della leadership detta il tono dell'organizzazione e aiuta a superare la potenziale resistenza al cambiamento.

Comunicazione trasparente

Mantieni una comunicazione aperta e trasparente con i dipendenti per tutto il processo di implementazione di Zero Trust. Spiega le motivazioni, i vantaggi e i risultati attesi dall'adozione e risolvi tempestivamente i dubbi. Fornisci aggiornamenti regolari sullo stato di avanzamento dell'implementazione. Ciò aumenterà il consenso, ridurrà la resistenza e creerà fiducia.

Sviluppo delle competenze e formazione

Una volta allineata la leadership stabilita la comunicazione, è importante sviluppare le competenze e le conoscenze dei dipendenti che implementeranno Zero Trust. Ciò include la comprensione dei principi di Zero Trust, le modalità per implementarli nel proprio lavoro e come rispondere agli eventi di sicurezza. Offri opportunità di formazione e sviluppo per aiutare i dipendenti ad acquisire queste competenze.

Conoscenze e competenze relative al cloud

Valuta le competenze e le lacune nelle conoscenze dell'organizzazione rispetto alle tecnologie cloud e ai principi di Zero Trust. Offri programmi di formazione e sviluppo per migliorare le competenze dei dipendenti e fornirgli le competenze necessarie per lavorare con efficacia in un ambiente Zero Trust incentrato sul cloud. Per stare al passo con l'evoluzione delle tecnologie e delle pratiche di sicurezza, promuovi una cultura dell'apprendimento continuo.

Cultura e consapevolezza della sicurezza

Valuta la cultura della sicurezza dell'organizzazione. Valuta il livello di consapevolezza della sicurezza tra i dipendenti, la loro comprensione delle best practice di sicurezza e la loro aderenza a policy e procedure. Identifica eventuali lacune nelle conoscenze sulla sicurezza. Prendi in considerazione la possibilità di condurre programmi di formazione sulla sensibilizzazione alla sicurezza per istruire i dipendenti sull'importanza di Zero Trust e sul loro ruolo nel mantenere un ambiente sicuro.

Struttura e ruoli organizzativi

Per implementare con successo Zero Trust, è necessario stabilire una struttura organizzativa e dei ruoli efficaci. Ciò include la creazione di un Cloud Center of Excellence (CCoE), la revisione e la modifica delle operazioni di sicurezza e l'assegnazione di ruoli e responsabilità per la gestione delle vulnerabilità, la risposta agli incidenti e il monitoraggio della sicurezza.

Centro di eccellenza del Cloud

Stabilisci una CCo E per fornire linee guida, best practice e supervisione per le operazioni cloud. A CCo E è un team o un gruppo di individui responsabili della creazione e dell'implementazione di best practice, linee guida e politiche di governance relative al cloud. La CCo E dovrebbe includere rappresentanti di diverse unità aziendali e team IT per contribuire a garantire la collaborazione e

l'allineamento. La CCo E svolge un ruolo cruciale nel promuovere l'adozione dei principi Zero Trust nei carichi di lavoro ospitati sul cloud. La CCo E facilita anche la condivisione delle conoscenze all'interno dell'organizzazione.

Operazioni di sicurezza

Per soddisfare le esigenze di un ambiente Zero Trust, rivedi e modifica l'attuale organizzazione delle operazioni di sicurezza. Per migliorare le capacità di monitoraggio, risposta agli incidenti e intelligence sulle minacce, prendi in considerazione l'implementazione di centri operativi di sicurezza (SOCs) o fornitori di servizi di sicurezza gestiti (MSSPs). Stabilisci ruoli e responsabilità per la gestione delle vulnerabilità, la risposta agli incidenti e il monitoraggio della sicurezza. Un processo di risposta agli incidenti ben funzionante è fondamentale per garantire il rilevamento e la correzione tempestiva degli eventi di sicurezza minori per interrompere l'evolversi degli eventi. Questo aiuta a evitare che un evento di scarsa rilevanza si trasformi in un evento di maggiore impatto.

Infrastruttura e architettura IT

Esamina l'architettura e l'infrastruttura IT della tua azienda per trovare eventuali vincoli o dipendenze che potrebbero influire sull'adozione di un approccio Zero Trust. Determina se le applicazioni e i sistemi attuali sono compatibili con i componenti dell'architettura Zero Trust necessari. Stabilisci se sono necessari miglioramenti o adeguamenti dell'infrastruttura per supportare la corretta implementazione dei principi di Zero Trust. Per ogni applicazione o sistema, valuta se è più opportuno implementare Zero Trust a livello individuale o attraverso uno sforzo di modernizzazione più ampio.

Gestione del rischio, governance e controllo delle modifiche

Per implementare con successo Zero Trust, stabilisci processi efficaci di gestione del rischio, governance e controllo delle modifiche. Ciò include l'allineamento della gestione del rischio ai principi di Zero Trust, lo sviluppo di un piano di risposta agli incidenti, la collaborazione con i dipartimenti legali e di conformità e l'istituzione di un processo di controllo delle modifiche.

Gestione del rischio

Esamina la strategia di gestione del rischio in atto nella tua azienda e stabilisci in quale misura aderisce ai principi di Zero Trust. Analizza l'efficienza degli attuali sistemi di risposta agli incidenti, delle misure di sicurezza e delle procedure di valutazione del rischio. Determina quali aree devono essere migliorate per conformarsi alla strategia Zero Trust. Inizia a sviluppare un sistema

automatizzato di risposta agli incidenti o un framework di monitoraggio e analisi continui per accelerare la risoluzione.

Processi di controllo delle modifiche

Per garantire che tutte le modifiche relative al cloud rispettino i requisiti di sicurezza e conformità, stabilisci metodi efficaci di controllo delle modifiche. Stabilisci una procedura sistematica di gestione delle modifiche che includa l'analisi della configurazione di sicurezza, le valutazioni dei rischi, le approvazioni e la documentazione. Rivedi e controlla frequentemente gli aggiornamenti per preservare l'integrità dell'architettura Zero Trust.

Monitoraggio e valutazione

Per implementare con successo Zero Trust, l'organizzazione deve monitorare e valutare continuamente il proprio assetto di sicurezza. Ciò include la definizione di indicatori chiave di performance (KPIs), il monitoraggio e la KPIs valutazione e la promozione di una cultura del miglioramento continuo. Seguendo questi passaggi, le organizzazioni possono garantire il successo dell'implementazione di Zero Trust e il proprio impegno continuo per migliorare l'assetto di sicurezza.

Indicatori chiave delle prestazioni

Stabilisci indicatori chiave di performance pertinenti (KPIs) per valutare il successo e l'efficacia dell'implementazione di Zero Trust. Questi KPIs potrebbero misurare la soddisfazione degli utenti, i progressi delle apparecchiature e dell'implementazione, la riduzione dei costi, il rispetto della conformità e il numero di eventi di sicurezza. Per monitorare lo sviluppo complessivo e trovare opportunità di miglioramento, monitoratele e valutatele regolarmente. KPIs

Miglioramento continuo

La creazione di sistemi per ottenere opinioni e approfondimenti dalle parti interessate contribuirà a promuovere una cultura del miglioramento continuo. Incoraggia i membri dello staff a condividere opinioni e proposte per migliorare la sicurezza, l'efficacia e l'esperienza utente dell'ambiente cloud. Utilizza questi feedback per semplificare le procedure, migliorare le misure di sicurezza e stimolare l'innovazione.

Riepilogo della sezione

Rispondendo a queste considerazioni organizzative e culturali, l'organizzazione può promuovere un ambiente favorevole all'adozione di un modello di sicurezza Zero Trust sul cloud. La sezione

successiva esplora gli approcci di adozione graduale, fornendo indicazioni su come implementare gradualmente i principi di Zero Trust in modo pratico e gestibile.

Coltivare una mentalità Zero Trust

L'implementazione di Zero Trust va oltre le implementazioni tecniche. Richiede un cambiamento culturale all'interno dell'organizzazione. Promuovere una mentalità Zero Trust implica l'enfasi sui seguenti aspetti chiave.

Istruzione e formazione Zero Trust

Istruisci i dipendenti sui valori e i vantaggi dell'architettura Zero Trust (ZTA). Fornisci spiegazioni tecniche e non tecniche dei concetti e degli approcci ZTA attraverso sessioni di formazione, workshop e altre risorse. Incoraggia i membri dello staff a essere consapevoli delle proprie responsabilità nello stabilire e sostenere un paradigma di sicurezza Zero Trust.

Collaborazione e comunicazione

Promuovi la collaborazione e la trasparenza tra tutti i team e i reparti coinvolti nell'implementazione di ZTA. Per garantire che tutti abbiano una conoscenza approfondita del piano, promuovi la comunicazione interfunzionale, la condivisione delle conoscenze e lo scambio di informazioni. Crea una cultura della responsabilità condivisa in cui tutti riconoscano l'importanza del proprio contributo alla sicurezza generale dell'azienda.

Apprendimento e miglioramento continui

Dai priorità all'apprendimento e al miglioramento continui nel contesto di Zero Trust. Incoraggia i dipendenti a rimanere aggiornati sulle ultime tendenze, tecnologie e best practice in materia di sicurezza. Promuovi una cultura dell'innovazione e della sperimentazione in cui i dipendenti siano incoraggiati a esplorare nuove soluzioni e approcci per rafforzare il livello di sicurezza dell'organizzazione.

Metriche e responsabilità

Stabilisci metriche e meccanismi di responsabilità chiari per misurare l'efficacia della strategia Zero Trust. Definisci gli indicatori chiave di performance (KPIs) in linea con gli obiettivi di sicurezza dell'organizzazione e monitora regolarmente i progressi. Ritenete gli individui e i team responsabili del loro contributo all'implementazione e al mantenimento dei principi Zero Trust.

Riepilogo della sezione

Affrontando questi aspetti e coltivando una mentalità Zero Trust, le organizzazioni possono creare una solida base per l'adozione e l'implementazione di successo di Zero Trust. Questo cambiamento culturale è essenziale per aiutare tutti i membri dell'organizzazione a comprendere l'importanza di Zero Trust e contribuire attivamente al suo successo.

La sezione successiva esplora gli approcci di adozione graduale, fornendo indicazioni su come implementare gradualmente i principi di Zero Trust in modo pratico e gestibile.

Approccio graduale a Zero Trust

L'adozione di un'architettura Zero Trust (ZTA) richiede un'attenta pianificazione e un'implementazione accurata. Consigliamo un approccio di adozione graduale per facilitare la transizione e ridurre al minimo le interruzioni delle operazioni aziendali. Questa sezione fornisce indicazioni sulle fasi principali dell'adozione di una ZTA.

Fase 1: valutazione e pianificazione

La prima fase dell'implementazione di Zero Trust consiste nella valutazione e nella pianificazione. Questa fase è fondamentale per il successo dell'implementazione nel suo complesso, poiché implica l'identificazione e la risoluzione di eventuali lacune nell'attuale assetto di sicurezza dell'organizzazione. Dedicando del tempo alla valutazione dello stato attuale e alla definizione degli obiettivi di sicurezza, è possibile gettare le basi per il successo dell'implementazione di Zero Trust.

Allo stesso tempo, una valutazione completa e accurata in ogni dettaglio non sempre potrebbe essere realistica. Per evitare un arenamento nella fase dell'analisi che impedisca di passare alle fasi successive, preparati a suddividere le analisi in compartimenti o ad accettare un certo grado di imperfezione.

1. Valuta lo stato attuale: esegui una valutazione dell'infrastruttura, delle policy e dei controlli di sicurezza esistenti. Identifica potenziali vulnerabilità, lacune nella sicurezza e aree che possono trarre giovamento dal l'implementazione dei principi di Zero Trust.
2. Definisci gli obiettivi di sicurezza: sulla base dei risultati della valutazione dello stato attuale, definisci obiettivi di sicurezza in linea con i principi di Zero Trust. Questi obiettivi di sicurezza, inoltre, devono essere in linea con la strategia di sicurezza generale dell'organizzazione e risolvere le vulnerabilità e le lacune identificate.
3. Progetta l'architettura: sviluppa una ZTA che supporti gli obiettivi di sicurezza della tua organizzazione. Questa architettura dovrebbe includere i componenti necessari, come soluzioni di gestione delle identità e degli accessi, meccanismi di segmentazione della rete e sistemi di monitoraggio continuo. L'architettura dovrebbe inoltre essere scalabile, adattabile e in grado di adattarsi alla crescita e ai progressi tecnologici futuri. Idealmente, questa architettura dovrebbe essere rappresentata in un formato facilmente utilizzabile dai team responsabili della sua implementazione, ad esempio un modello AWS CloudFormation , e non soltanto come documento o diagramma.

4. Coinvolgi le parti interessate: coinvolgi tutte le parti interessate, comprese le unità aziendali, i team IT e i team di sicurezza, per ottenere informazioni e allineare i rispettivi obiettivi al piano di implementazione della ZTA. Incoraggia la collaborazione e la comunicazione per stabilire una comprensione condivisa dei vantaggi e dei requisiti dell'approccio Zero Trust.

Fase 2: sperimentazione e implementazione

La seconda fase dell'implementazione di Zero Trust consiste nella sperimentazione e nell'implementazione. Questa fase prevede il test della ZTA in un ambiente controllato su piccola scala e la successiva implementazione iterativa in tutta l'organizzazione. È importante istruire i dipendenti sulle nuove misure di sicurezza e sul loro ruolo nel mantenere un ambiente Zero Trust.

1. Esegui un'implementazione pilota: testa la ZTA in un ambiente controllato su piccola scala. Implementa i componenti e i controlli di sicurezza necessari definiti nella fase di progettazione dell'architettura. Monitora attentamente l'implementazione pilota, raccogli feedback e apporta le modifiche necessarie. Cerca di essere flessibile nelle fasi iniziali del processo, quando l'approccio Zero Trust si trasforma da un esercizio teorico a uno pratico per realizzare un'esperienza concreta.
2. Implementa in modo iterativo: utilizzando le lezioni apprese dall'implementazione pilota di Zero Trust, inizia a distribuirlo in modo iterativo in tutta l'organizzazione. Crea slancio attraverso un effetto volano che non richieda un intervento esteso per raggiungere una massa critica di implementazioni. Quando necessario, posticipa i mandati o le escalation di livello dirigenziale alla fase successiva dell'implementazione.
3. Forma e sensibilizza gli utenti: istruisci i dipendenti sulle nuove misure di sicurezza e sul loro ruolo nel mantenere un ambiente Zero Trust. Sottolinea l'importanza di pratiche sicure, come password complesse, autenticazione a più fattori e aggiornamenti di sicurezza regolari.
4. Gestisci il cambiamento: crea un piano completo di gestione delle modifiche per affrontare i cambiamenti organizzativi e culturali associati all'adozione di Zero Trust. Comunica ai dipendenti i vantaggi e le motivazioni alla base dell'adozione e affronta eventuali dubbi o resistenze. Fornisci supporto e assistenza continui per facilitare una transizione senza intoppi.

Fase 3: monitoraggio e miglioramento continuo

La terza e ultima fase dell'implementazione di Zero Trust consiste nel monitoraggio e nel miglioramento continuo. Questa fase prevede l'istituzione di un programma completo di monitoraggio

e analisi, la creazione di un piano completo di risposta agli incidenti e la richiesta di feedback regolari da parte delle parti interessate e degli utenti.

1. Monitora in modo continuativo: stabilisci un programma completo di monitoraggio e analisi per valutare l'assetto di sicurezza e rilevare eventuali anomalie potenziali in modo continuativo. Utilizza strumenti e tecnologie di sicurezza avanzati per monitorare il comportamento degli utenti, il traffico di rete e le attività del sistema.
2. Pianifica la risposta e la correzione degli incidenti: crea un piano completo di risposta agli incidenti in linea con i principi di Zero Trust. Stabilisci percorsi di risoluzione chiari, definisci ruoli e responsabilità e implementa meccanismi automatici di risposta agli incidenti, ove possibile. Testa e aggiorna regolarmente il piano di risposta agli incidenti.
3. Ottieni feedback e valutazioni: richiedi regolarmente il feedback delle parti interessate e degli utenti per raccogliere informazioni sull'efficacia dell'architettura Zero Trust (ZTA). Conduci valutazioni periodiche per misurare l'impatto sull'assetto di sicurezza, sull'efficienza operativa e sull'esperienza dell'utente. Utilizza i feedback e i risultati della valutazione per identificare le aree di miglioramento. Aspettatevi cambiamenti nel tempo e considerate in che modo i team di sviluppo implementeranno questi aggiornamenti con il minimo sforzo o interruzioni. ZTAs

Riepilogo della sezione

Seguendo questo approccio di adozione graduale, le organizzazioni possono passare a una ZTA in modo efficace riducendo al minimo i rischi e le interruzioni. La sezione successiva illustra le migliori pratiche per raggiungere il successo con l'implementazione di Zero Trust, illustrando considerazioni e raccomandazioni chiave per i dirigenti e CxOs i VPs senior manager.

Le best practice per raggiungere il successo con Zero Trust

Il successo dell'adozione dell'architettura Zero Trust (ZTA) richiede un approccio strategico e il rispetto di alcune best practice. Questa sezione presenta una serie di best practice per guidare e guidare CxOs i VPs senior manager nel raggiungimento del successo con l'adozione di Zero Trust. Seguendo questi consigli, la tua organizzazione può stabilire una solida base di sicurezza e sfruttare i vantaggi di un approccio Zero Trust:

- Definisci obiettivi e risultati aziendali chiari: definisci chiaramente gli obiettivi e i risultati aziendali attesi per le operazioni cloud. Allinea questi obiettivi ai principi di Zero Trust per creare una solida base di sicurezza e sostenere al contempo la crescita e l'innovazione del business.
- Esegui una valutazione completa: esegui una valutazione completa dell'attuale infrastruttura IT, delle applicazioni e delle risorse di dati. Identifica le dipendenze, il debito tecnico e i potenziali problemi di compatibilità. Questa valutazione costituirà la base per il piano di adozione e contribuirà a stabilire le priorità dei carichi di lavoro in base a criticità, complessità e impatto aziendale.
- Sviluppa un piano di adozione: incorpora un piano di adozione dettagliato che delinea l' step-by-stepapproccio per lo spostamento di carichi di lavoro, applicazioni e dati sul cloud. Definisci le fasi, le tempistiche e le dipendenze relative all'adozione. Coinvolgi le principali parti interessate e alloca le risorse di conseguenza.
- Inizia a sviluppare da subito: la tua abilità nel rappresentare fedelmente l'implementazione di Zero Trust nella tua organizzazione crescerà significativamente quando passerai dalla teoria alla pratica, sviluppandolo e mettendolo in atto, piuttosto che limitarti solo a esaminarlo e discuterne.
- Ottieni la sponsorizzazione esecutiva: assicurati il supporto e la sponsorizzazione esecutiva per l'implementazione di Zero Trust. Coinvolgi altri dirigenti al massimo livello esecutivo per sostenere l'iniziativa e allocare le risorse necessarie. L'impegno dei dirigenti è essenziale per promuovere i cambiamenti culturali e organizzativi necessari per il successo dell'implementazione.
- Implementa un framework di governance: crea un framework di governance che definisca ruoli, responsabilità e processi decisionali per l'implementazione di Zero Trust. Definisci chiaramente la responsabilità e la titolarità dei controlli di sicurezza, della gestione del rischio e della conformità. Rivedi e aggiorna regolarmente il framework di governance per adattarlo all'evoluzione dei requisiti di sicurezza.
- Supporta la collaborazione interfunzionale: incoraggia la collaborazione e la comunicazione tra diverse unità aziendali, team IT e team di sicurezza. Crea una cultura della responsabilità condivisa per promuovere l'allineamento e il coordinamento durante l'implementazione di Zero

Trust. Promuovi le interazioni frequenti, la condivisione delle conoscenze e la risoluzione collettiva dei problemi.

- Proteggi i tuoi dati e le tue applicazioni: Zero Trust non riguarda solo l'accesso degli utenti finali a risorse e applicazioni. I principi di Zero Trust devono essere implementati anche all'interno e tra i carichi di lavoro. Applica gli stessi principi tecnici (identità avanzata, microsegmentazione e autorizzazione) sfruttando anche tutto il contesto disponibile all'interno del data center.
- Fornisci una difesa approfondita: implementa una defense-in-depth strategia utilizzando più livelli di controlli di sicurezza. Combina diverse tecnologie di sicurezza, come l'autenticazione a più fattori (MFA), la segmentazione della rete, la crittografia e il rilevamento delle anomalie, per fornire una protezione completa. Assicurati che ogni livello sia complementare agli altri per creare un sistema di difesa affidabile.
- Richiedi un'autenticazione avanzata: applica meccanismi di autenticazione avanzati, come l'MFA, per tutti gli utenti che accedono a ogni tipo di risorsa. Idealmente, prendi in considerazione l'MFA moderna, come le chiavi di sicurezza FIDO2 basate su hardware, che forniscono un elevato livello di garanzia di autenticazione per Zero Trust e offrono ampi vantaggi in termini di sicurezza (ad esempio, protezione dal phishing).
- Centralizza e migliora l'autorizzazione: autorizza in modo specifico ogni tentativo di accesso. A seconda delle specifiche del protocollo, questa operazione deve essere eseguita in base alla connessione o alla richiesta. La soluzione ideale è quella basata sulla richiesta. Sfrutta tutto il contesto disponibile, tra cui informazioni su identità, dispositivo, comportamento e rete per prendere decisioni di autorizzazione più granulari, adattive e sofisticate.
- Adotta il principio del privilegio minimo: implementa il principio del privilegio minimo per concedere agli utenti i diritti di accesso minimi necessari per svolgere le proprie mansioni lavorative. Rivedi e aggiorna regolarmente le autorizzazioni di accesso in base a ruoli lavorativi, responsabilità ed esigenze aziendali. Implementa la fornitura degli accessi. just-in-time
- Utilizza la gestione degli accessi privilegiati: implementa una soluzione di gestione degli accessi privilegiati (PAM) per proteggere gli account privilegiati e ridurre il rischio di accesso non autorizzato ai sistemi critici. Le soluzioni PAM possono fornire controlli degli accessi privilegiati, registrazione delle sessioni e funzionalità di controllo per aiutare l'organizzazione a proteggere i dati e i sistemi più sensibili.
- Utilizza la microsegmentazione: suddividi la rete in segmenti più piccoli e isolati. Impiega la microsegmentazione per applicare controlli di accesso rigorosi tra i segmenti in base ai ruoli degli utenti, alle applicazioni o alla sensibilità dei dati. Cerca di eliminare tutti i percorsi di rete non necessari, in particolare quelli che portano ai dati.

- Monitora e rispondi agli avvisi di sicurezza: implementa un programma completo di monitoraggio della sicurezza e risposta agli incidenti nell'ambiente cloud. Utilizza strumenti e servizi di sicurezza nativi del cloud per rilevare le minacce in tempo reale, analizzare i log e automatizzare la risposta agli incidenti. Stabilisci procedure chiare di risposta agli incidenti, esegui valutazioni di sicurezza a cadenza regolare e monitora continuamente eventuali anomalie o attività sospette.
- Utilizza il monitoraggio continuo: per rilevare e rispondere agli incidenti di sicurezza in modo rapido ed efficace, implementa il monitoraggio continuo. Utilizza strumenti di analisi della sicurezza avanzati per monitorare il comportamento degli utenti, il traffico di rete e le attività del sistema. Automatizza gli avvisi e le notifiche per garantire che gli incidenti ricevano una risposta tempestiva.
- Promuovi una cultura della sicurezza e della conformità: promuovi una cultura della sicurezza e della conformità in tutta l'organizzazione. Informa i dipendenti sulle best practice di sicurezza, sul loro ruolo nel mantenere un ambiente cloud sicuro e sull'importanza di aderire ai principi di Zero Trust. Conduci regolarmente corsi di sensibilizzazione alla sicurezza per garantire che i dipendenti prestino attenzione ai tentativi di ingegneria sociale e che comprendano le proprie responsabilità in materia di privacy e protezione dei dati.
- Utilizza simulazioni di ingegneria sociale: esegui simulazioni di ingegneria sociale per valutare la suscettibilità degli utenti agli attacchi di ingegneria sociale. Utilizza i risultati delle simulazioni peri personalizzare i programmi di formazione, con l'obiettivo di migliorare la consapevolezza degli utenti e la risposta alle potenziali minacce.
- Promuovi la formazione continua: instaura una cultura della formazione e dell'apprendimento continui fornendo continuamente formazione e risorse in materia di sicurezza. Aggiorna regolarmente gli utenti in merito all'evoluzione delle best practice di sicurezza. Incoraggia gli utenti a rimanere vigili e a segnalare tempestivamente eventuali attività sospette.
- Valuta e ottimizza in modo continuativo: valuta regolarmente l'ambiente cloud per individuare le aree di miglioramento. Utilizza strumenti nativi del cloud per monitorare l'utilizzo delle risorse e le prestazioni e condurre valutazioni delle vulnerabilità e test di penetrazione (pen-test) per identificare e risolvere eventuali punti deboli.
- Stabilisci un framework di governance e conformità: sviluppa un framework di governance e conformità per assicurarti che l'organizzazione sia in linea con gli standard di settore e i requisiti normativi. All'interno del framework, definisci policy, procedure e controlli per proteggere dati e sistemi dall'accesso, dall'uso, dalla divulgazione, dall'interruzione, dalla modifica o dalla distruzione non autorizzati. Implementa sistemi per il monitoraggio e la rendicontazione dei parametri di conformità, effettuando audit periodici e intervenendo prontamente per risolvere qualsiasi problema di non conformità che dovesse emergere.

- Incoraggia la collaborazione e la condivisione delle conoscenze: incoraggia la collaborazione e la condivisione delle conoscenze tra i team coinvolti nell'adozione della ZTA. A tale scopo, promuovi la comunicazione e la collaborazione interfunzionali tra team IT, team di sicurezza e altre unità aziendali. L'organizzazione può anche programmare forum, workshop e sessioni di condivisione delle conoscenze per promuovere la comprensione, affrontare le sfide e condividere le lezioni apprese durante il processo di adozione.

Punti principali

Questa guida ha esplorato gli aspetti essenziali dello sviluppo di una strategia Zero Trust Architecture (ZTA) di successo. Questa sezione riassume i punti principali delle linee guida prescrittive presentate:

- Comprendi i principi di Zero Trust: Zero Trust è un modello concettuale e l'insieme dei meccanismi associati che si concentrano sull'offerta di controlli di sicurezza delle risorse digitali che non dipendono in modo esclusivo o fondamentale dai controlli di rete o dai perimetri di rete tradizionali. Al contrario, i controlli di rete incorporano elementi relativi alle identità, ai dispositivi, ai comportamenti e ad altri segnali e aspetti contestuali per prendere decisioni di accesso più granulari, intelligenti e adattive su base continuativa. Acquisisci familiarità con i principi fondamentali di Zero Trust, come il privilegio minimo, la microsegmentazione, l'autenticazione continua e l'autorizzazione adattiva.
- Definisci obiettivi chiari: definisci chiaramente gli obiettivi e i risultati aziendali attesi dall'adozione di una ZTA. Allinea questi obiettivi ai principi di Zero Trust per agevolare la creazione di una solida base di sicurezza, favorendo al contempo la crescita e l'innovazione del business.
- Conduci valutazioni complete: esegui una valutazione approfondita dell'infrastruttura IT, delle applicazioni e delle risorse di dati esistenti. Identifica le dipendenze, i debiti tecnici e i problemi di compatibilità per definire la strategia di adozione.
- Sviluppa un piano di adozione ZTA: crea un piano dettagliato che delinei l' step-by-stepapproccio per lo spostamento di carichi di lavoro, applicazioni e dati sul cloud. Prendi in considerazione fattori come i requisiti di conformità e la modernizzazione delle applicazioni.
- Implementa una ZTA solida: progetta e implementa una ZTA che applichi controlli granulari degli accessi, meccanismi avanzati di autenticazione e il monitoraggio continuo. Per un'adozione ZTA più efficiente, utilizza servizi Zero Trust nativi per il cloud, come Accesso verificato da AWS Amazon VPC Lattice.
- Dai priorità alla sicurezza dei dati e delle applicazioni: applica i principi di Zero Trust (identità avanzata, microsegmentazione e autorizzazione) per fornire tutto il contesto disponibile. Utilizza questo contesto per gli utenti che accedono a sistemi e risorse e per il flusso di comunicazioni e dati all'interno e tra i componenti di back-end.
- Stabilisci framework di monitoraggio e risposta agli incidenti: implementa solide funzionalità di monitoraggio della sicurezza e risposta agli incidenti nell'ambiente cloud. Utilizza strumenti di sicurezza nativi del cloud per il rilevamento delle minacce in tempo reale, l'analisi dei log e l'automazione della risposta agli incidenti, come Amazon Inspector AWS Security Hub e Amazon. GuardDuty

- Promuovi una cultura della sicurezza e della conformità: promuovi una cultura della consapevolezza e della conformità alla sicurezza in tutta l'organizzazione. Informa i dipendenti sulle best practice di sicurezza e sul loro ruolo nel mantenere un ambiente cloud sicuro.
- Valuta e ottimizza su base continuativa: valuta regolarmente l'ambiente cloud, i controlli di sicurezza e i processi operativi. Per raccogliere informazioni e ottimizzare l'utilizzo delle risorse, la gestione dei costi e le prestazioni, utilizza strumenti di analisi e monitoraggio nativi del cloud come Amazon e. CloudWatch AWS Security Hub
- Stabilisci framework di governance e conformità: sviluppa framework di governance e conformità in linea con gli standard di settore e i requisiti normativi. Definisci policy, procedure e controlli per garantire il rispetto degli standard di sicurezza, privacy e conformità.

Passaggi successivi

L'adozione di un'architettura Zero Trust (ZTA) è uno dei modi più sicuri per migliorare l'assetto dell'organizzazione e ridurre i rischi. Questo prontuario ti ha fornito una roadmap completa per l'implementazione di Zero Trust, dalla comprensione dei principi alla valutazione dello stato di preparazione, fino all'implementazione dei componenti necessari.

I passaggi successivi di questo flusso di lavoro o dominio prevedono le attività seguenti:

- Implementazione del piano di adozione
- Implementazione della ZTA
- Svolgimento di valutazioni di sicurezza a cadenza regolare
- Ottimizzazione continua dell'ambiente cloud e dei controlli di sicurezza

La ZTA è un processo continuo che richiede monitoraggio, valutazione e adattamento costanti per garantire basi di sicurezza solide. Seguendo le best practice descritte in questa guida, l'organizzazione può migliorare il proprio assetto di sicurezza, garantire la conformità alle normative e proteggere i dati sensibili.

Domande frequenti

Questa sezione fornisce le risposte alle domande più frequenti sulla progettazione e sull'implementazione di un'architettura Zero Trust (ZTA).

Che cos'è Zero Trust?

Zero Trust è un modello concettuale e l'insieme dei meccanismi associati che si concentrano sull'offerta di controlli di sicurezza delle risorse digitali che non dipendono in modo esclusivo o fondamentale dai controlli di rete o dai perimetri di rete tradizionali. Al contrario, i controlli di rete incorporano elementi relativi alle identità, ai dispositivi, ai comportamenti e ad altri segnali e aspetti contestuali per prendere decisioni di accesso più granulari, intelligenti e adattive su base continuativa.

Cosa Servizi AWS può aiutarmi a implementare l'architettura Zero Trust?

AWS offre diversi servizi che possono contribuire all'implementazione di Zero Trust, come AWS Identity and Access Management (IAM) Accesso verificato da AWS, Amazon Virtual Private Cloud (Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway e Amazon. GuardDuty

Come posso garantire un'adeguata protezione dei dati con AWS?

AWS offre servizi come AWS Key Management Service (AWS KMS) per la crittografia dei dati a riposo e in transito, Amazon Virtual Private Cloud (Amazon VPC) per l'isolamento della rete e per l'archiviazione e AWS Secrets Manager il recupero sicuri delle credenziali.

Può AWS aiutarti con i requisiti di conformità in un ambiente Zero Trust?

Sì, AWS dispone di programmi e servizi di conformità che aiutano a soddisfare vari requisiti normativi. AWS Artifact fornisce l'accesso ai report di AWS conformità e AWS Config supporta il monitoraggio e la valutazione continui della conformità.

Esistono AWS strumenti o servizi per automatizzare la sicurezza in un ambiente Zero Trust?

AWS fornisce servizi come AWS Security Hub, ad esempio, che centralizzano e automatizzano i risultati di sicurezza e AWS Config regole per la definizione e l'applicazione delle politiche di sicurezza.

Come posso garantire il monitoraggio continuo e la risposta agli incidenti in un ambiente cloud Zero Trust con AWS

AWS offre servizi come Amazon CloudWatch per il monitoraggio in tempo reale e AWS CloudTrail per la registrazione e l'analisi. Per le best practice di risposta agli incidenti, puoi utilizzare la Guida alla risposta agli incidenti di sicurezza AWS .

Risorse

Riferimenti

- What is a cloud center of excellence and why should your organization create one? — Questo post sul blog fornisce una panoramica di CCo E, le migliori pratiche per creare una CCo E efficace e altro ancora.
- Zero Trust on AWS: questa pagina fornisce una panoramica dei principi di sicurezza Zero Trust e delle migliori pratiche nell' AWS ambiente.
- Architettura Zero Trust: una AWS prospettiva — Questo post sul blog condivide una definizione e i principi guida del modo in cui Zero Trust viene implementato AWS.
- AWS Identity and Access Management (IAM) Guida per l'utente: questa guida offre una documentazione completa sulla gestione degli accessi e delle autorizzazioni degli utenti in IAM, un componente fondamentale dell'architettura Zero Trust.
- AWS Security Hub— Scopri Security Hub, un servizio che fornisce una visione completa degli avvisi di sicurezza e dello stato di conformità in tutto il Account AWS mondo.
- Framework AWS Well-Architected: esplora il Framework Well-Architected, che fornisce indicazioni sulla creazione di architetture sicure, resilienti, efficienti e dalle prestazioni elevate su AWS.
- AWS Guida alla risposta agli incidenti di sicurezza: questa guida presenta una panoramica dei fondamenti della risposta agli incidenti di sicurezza all'interno dell'ambiente aziendale. Cloud AWS Fornisce una panoramica dei concetti di sicurezza del cloud e di risposta agli incidenti e identifica le funzionalità, i servizi e i meccanismi cloud a disposizione dei clienti che devono rispondere a problemi di sicurezza.

Strumenti

- Gateway Amazon API
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty

- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub
- Accesso verificato da AWS

Cronologia dei documenti

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

Modifica	Descrizione	Data
Aggiornamenti aggiunti	Sono state aggiunte informazioni alla sezione Componenti chiave di un'architettura Zero Trust, sono state apportate modifiche alla sezione Valutazione della preparazione dell'organizzazione all'adozione di Zero Trust, sono state aggiunte informazioni alla sezione Best practice e sono state apportate modifiche alle domande frequenti.	4 dicembre 2023
Pubblicazione iniziale	—	19 giugno 2023

AWS Glossario delle linee guida prescrittive

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

Numeri

7 R

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

- Rifattorizzare/riprogettare: trasferisci un'applicazione e modifica la sua architettura sfruttando appieno le funzionalità native del cloud per migliorare l'agilità, le prestazioni e la scalabilità. Ciò comporta in genere la portabilità del sistema operativo e del database. Esempio: migra il tuo database Oracle locale all'edizione compatibile con Amazon Aurora PostgreSQL.
- Ridefinire la piattaforma (lift and reshape): trasferisci un'applicazione nel cloud e introduci un certo livello di ottimizzazione per sfruttare le funzionalità del cloud. Esempio: migra il tuo database Oracle locale ad Amazon Relational Database Service (Amazon RDS) per Oracle in. Cloud AWS
- Riacquistare (drop and shop): passa a un prodotto diverso, in genere effettuando la transizione da una licenza tradizionale a un modello SaaS. Esempio: migra il tuo sistema di gestione delle relazioni con i clienti (CRM) su Salesforce.com.
- Eseguire il rehosting (lift and shift): trasferisci un'applicazione sul cloud senza apportare modifiche per sfruttare le funzionalità del cloud. Esempio: migra il database Oracle locale su Oracle su un'istanza in. EC2 Cloud AWS
- Trasferire (eseguire il rehosting a livello hypervisor): trasferisci l'infrastruttura sul cloud senza acquistare nuovo hardware, riscrivere le applicazioni o modificare le operazioni esistenti. Si esegue la migrazione dei server da una piattaforma locale a un servizio cloud per la stessa piattaforma. Esempio: migra un'applicazione suMicrosoft Hyper-V. AWS
- Riesaminare (mantenere): mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a un momento successivo e applicazioni legacy che desideri mantenere, perché non vi è alcuna giustificazione aziendale per effettuarne la migrazione.
- Ritirare: disattiva o rimuovi le applicazioni che non sono più necessarie nell'ambiente di origine.

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

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

migrazione attiva-passiva

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

funzione aggregata

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

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

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

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

AWS Workload Qualification Framework (WQF)AWS

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

B

bot difettoso

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

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

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

Classificazione binaria

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

filtro Bloom

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

distribuzioni blu/verdi

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

bot

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

botnet

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

ramo

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

accesso break-glass

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

strategia brownfield

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

cache del buffer

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

capacità di business

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

pianificazione della continuità operativa (BCP)

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

C

CAF

Vedi AWS Cloud Adoption Framework.

implementazione canaria

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

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

Centro di eccellenza cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

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

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

CMDB

Vedi database di gestione della configurazione.

repository di codice

Una posizione in cui il codice di origine e altri asset, come documentazione, esempi e script, vengono archiviati e aggiornati attraverso processi di controllo delle versioni. Gli archivi cloud più comuni includono GitHub oBitbucket Cloud. Ogni versione del codice è denominata ramo. In una

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

cache fredda

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

dati freddi

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

visione artificiale (CV)

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

deriva della configurazione

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

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

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

CDpuò aiutarvi ad automatizzare i processi, migliorare la produttività, migliorare la qualità del codice e velocizzare le consegne. Per ulteriori informazioni, consulta Vantaggi della distribuzione continua. CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta Distribuzione continua e implementazione continua a confronto.

CV

Vedi visione artificiale.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

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

deriva dei dati

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

dati in transito

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

rete di dati

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di definizione del database.

deep ensemble

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

deep learning

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

defense-in-depth

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

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

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

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

gemello digitale

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

tabella delle dimensioni

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

disastro

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

disaster recovery (DR)

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

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

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

DOTT.

Vedi disaster recovery.

rilevamento della deriva

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

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

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

scambio elettronico di dati (EDI)

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

crittografia

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

chiave crittografica

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

endianità

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

endpoint

Vedi service endpoint.

servizio endpoint

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

pianificazione delle risorse aziendali (ERP)

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

crittografia envelope

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

ambiente

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

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

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

epica

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

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

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

F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

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

prompt con pochi scatti

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

Vedi il modello di base.

modello di fondazione (FM)

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

G

AI generativa

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

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

immagine dorata

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

strategia greenfield

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

guardrail

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

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

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

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

alta disponibilità (HA)

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

modernizzazione storica

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

dati di esclusione

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

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

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

I

IaC

Considera l'infrastruttura come codice.

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

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

VPC in ingresso (ingress)

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

migrazione incrementale

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

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

IIoInternet delle cose industriale (T)

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

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

modello linguistico di grandi dimensioni (LLM)

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

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

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

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

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

ramo principale

Vedi filiale.

malware

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

servizi gestiti

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

sistema di esecuzione della produzione (MES)

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

MAP

Vedi Migration Acceleration Program.

meccanismo

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

account membro

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

MEH.

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

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

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

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

migrazione su larga scala

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

fabbrica di migrazione

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

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

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

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

Vedi machine learning.

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

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

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

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

infrastruttura mutabile

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

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

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

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

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

OPC-UA

Vedi Open Process Communications - Unified Architecture.

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

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

tecnologia operativa (OT)

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

integrazione delle operazioni (OI)

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

trail organizzativo

Un percorso creato da noi AWS CloudTrail che registra tutti gli eventi di un'organizzazione per tutti Account AWS . AWS Organizations Questo percorso viene creato in ogni Account AWS che fa parte dell'organizzazione e tiene traccia dell'attività in ogni account. Per ulteriori informazioni, consulta Creazione di un percorso per un'organizzazione nella CloudTrail documentazione.

gestione del cambiamento organizzativo (OCM)

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

persone, a causa della velocità di cambiamento richiesta nei progetti di adozione del cloud. Per ulteriori informazioni, consultare la Guida OCM.

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

ORR

Vedi la revisione della prontezza operativa.

- NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

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

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

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

persistenza poliglotta

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

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

concatenamento rapido

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

pseudonimizzazione

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

publish/subscribe (pub/sub)

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

Q

Piano di query

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

regressione del piano di query

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

R

Matrice RACI

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

STRACCIO

Vedi Retrieval Augmented Generation.

ransomware

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

Matrice RASCI

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

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

Regione

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

regressione

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

riospitare

Vedi 7 R.

rilascio

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

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

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

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi l'obiettivo del punto di ripristino.

RTO

Vedi l'obiettivo del tempo di ripristino.

runbook

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

S

SAML 2.0

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

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

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

sicurezza fin dalla progettazione

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

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

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

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

Modello di responsabilità condivisa

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

SIEM

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

punto di errore singolo (SPOF)

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

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

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

SPOF

Vedi punto di errore singolo.

schema a stella

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

modello del fico strangolatore

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

sottorete

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

controllo di supervisione e acquisizione dati (SCADA)

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

crittografia simmetrica

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

test sintetici

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

prompt di sistema

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

T

tags

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

variabile di destinazione

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

elenco di attività

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

Ambiente di test

Vedi ambiente.

training

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

Transit Gateway

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

flusso di lavoro basato su trunk

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

Accesso attendibile

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

regolazione

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

team da due pizze

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

U

incertezza

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

compiti indifferenziati

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

ambienti superiori

Vedi ambiente.

V

vacuum

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

controllo delle versioni

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

Peering VPC

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

vulnerabilità

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

W

cache calda

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

dati caldi

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

funzione finestra

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

Carico di lavoro

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

flusso di lavoro

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

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

Z

exploit zero-day

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

vulnerabilità zero-day

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

prompt zero-shot

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

applicazione zombie

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

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