Controlli di sicurezza consigliati per l'implementazione delle funzionalità di sicurezza AWS CAF

AWS Guida prescrittiva

AWS Guida prescrittiva: Controlli di sicurezza consigliati per l'implementazione delle funzionalità di sicurezza AWS CAF

Table of Contents

Controlli di sicurezza consigliati per l'implementazione delle AWS funzionalità di sicurezza CAF

Rishi Singla e Rovan Omar, Amazon Web Services ()AWS

Novembre 2023 (cronologia dei documenti)

La sicurezza è la massima priorità in. AWS Per contribuire ad alleggerire il carico operativo, condividi la responsabilità della sicurezza e della conformità del cloud con AWS. AWS è responsabile della sicurezza del cloud, il che significa proteggere l'infrastruttura che gestisce i servizi offerti in Cloud AWS. L'utente è responsabile della sicurezza nel cloud, ad esempio dei dati e delle applicazioni. Questa guida fornisce controlli di sicurezza che possono aiutarti a soddisfare le tue responsabilità in materia di sicurezza in Cloud AWS.

Il AWS Cloud Adoption Framework (AWS CAF) fornisce le migliori pratiche progettate per migliorare la preparazione al cloud. AWS CAF classifica queste best practice in sei prospettive: business, persone, governance, piattaforma, sicurezza e operazioni. Questa guida si concentra sulle seguenti funzionalità dal punto di vista della sicurezza:

- Gestione delle identità e degli accessi: gestisci le identità umane e automatiche e le relative autorizzazioni su larga scala.
- Rilevamento delle minacce: configura la registrazione e il monitoraggio per rilevare e indagare su potenziali errori di configurazione, minaccia o comportamento imprevisto in materia di sicurezza.
- Protezione dell'infrastruttura: proteggi i sistemi e i servizi da accessi involontari o non autorizzati e da potenziali vulnerabilità.
- Protezione dei dati: categorizza i dati in base ai livelli di sensibilità. Mantieni la visibilità e il controllo sui dati e sul modo in cui sono accessibili e utilizzati nella tua organizzazione.
- Risposta agli incidenti: stabilisci meccanismi per rispondere e mitigare il potenziale impatto degli incidenti di sicurezza.

La mancata implementazione di controlli di sicurezza preventivi, investigativi e reattivi per queste funzionalità di sicurezza AWS CAF può rappresentare un rischio critico per l'ambiente cloud e interrompere l'attività. L'implementazione dei controlli di sicurezza descritti in questa guida può aiutare l'organizzazione a proteggere il proprio ambiente cloud.

> **Note**
>
> AWS fornisce servizi, strumenti e framework che possono aiutarti a operare in modo sicuro in. Cloud AWS Questa guida si allinea e integra il AWS Well-Architected Framework AWS , il Cloud Adoption Framework AWS (CAF), AWS la Security Reference Architecture AWS (SRA) e altre raccomandazioni sulla sicurezza pubblicate da. AWS I controlli di questa guida non comprendono tutte le considerazioni sulla sicurezza del cloud e questa guida non intende sostituire questi framework.

Raccomandazioni sul controllo della sicurezza per la gestione dell'identità e dell'accesso

È possibile creare identità in AWS o connettere una fonte di identità esterna. Tramite le policy AWS Identity and Access Management (IAM), concedi agli utenti le autorizzazioni necessarie in modo che possano accedere o gestire AWS risorse e applicazioni integrate. Una gestione efficace delle identità e degli accessi aiuta a verificare che le persone e le macchine giuste abbiano accesso alle risorse giuste nelle giuste condizioni. Il AWS Well-Architected Framework fornisce le migliori pratiche per la gestione delle identità e delle relative autorizzazioni. Esempi di best practice includono l'affidamento a un provider di identità centralizzato e l'utilizzo di potenti meccanismi di accesso, come l'autenticazione a più fattori (MFA). I controlli di sicurezza in questa sezione possono aiutarti a implementare queste best practice.

Controlli in questa sezione:

- Monitora e configura le notifiche per l'attività degli utenti root
- Non creare chiavi di accesso per l'utente root
- Abilita MFA per l'utente root
- Segui le best practice di sicurezza per IAM
- Concedi le autorizzazioni con il privilegio minimo
- Definisci le barriere di autorizzazione a livello di carico di lavoro
- Ruota le chiavi di accesso IAM a intervalli regolari
- Identifica le risorse condivise con un'entità esterna

Monitora e configura le notifiche per l'attività degli utenti root

La prima volta che si crea un Account AWS, si inizia con un'identità di accesso singolo denominata utente root. Per impostazione predefinita, l'utente root ha accesso completo a tutte Servizi AWS le risorse dell'account. È necessario controllare e monitorare attentamente l'utente root e utilizzarlo solo per le attività che richiedono le credenziali dell'utente root.

Per maggiori informazioni, consulta le seguenti risorse:

- Concedi l'accesso con il minimo privilegio nel Well-Architected Framework AWS
- Monitora l'attività degli utenti root di IAM in Prescriptive Guidance AWS

Non creare chiavi di accesso per l'utente root

L'utente root è l'utente più privilegiato in un Account AWS. La disabilitazione dell'accesso programmatico all'utente root aiuta a ridurre il rischio di esposizione involontaria delle credenziali dell'utente e la conseguente compromissione dell'ambiente cloud. Ti consigliamo di creare e utilizzare i ruoli IAM come credenziali temporanee per accedere alle tue risorse e alle tue. Account AWS

Per maggiori informazioni, consulta le seguenti risorse:

- La chiave di accesso utente root IAM non dovrebbe esistere nella documentazione AWS Security Hub CSPM
- Eliminazione delle chiavi di accesso per l'utente root nella documentazione IAM
- Ruoli IAM nella documentazione IAM

Abilita MFA per l'utente root

Ti consigliamo di abilitare più dispositivi di autenticazione a più fattori (MFA) per Account AWS l'utente root e gli utenti IAM. Ciò aumenta il livello di sicurezza Account AWS e può semplificare la gestione degli accessi. Poiché un utente root è un utente altamente privilegiato in grado di eseguire azioni privilegiate, è fondamentale richiedere l'autenticazione MFA per l'utente root. È possibile utilizzare un dispositivo MFA hardware che genera un codice numerico basato sull'algoritmo TOTP (Time-based One-Time Password), una chiave di sicurezza hardware FIDO o un'applicazione di autenticazione virtuale.

Nel 2024, l'MFA sarà richiesta per accedere all'utente root di qualsiasi utente. Account AWS Per ulteriori informazioni, consulta Secure by Design: AWS to enhance MFA requirements in 2024 nel Security Blog. AWS Ti consigliamo vivamente di estendere questa pratica di sicurezza e richiedere l'autenticazione MFA per tutti i tipi di utenti nei tuoi AWS ambienti.

Se possibile, si consiglia di utilizzare un dispositivo MFA hardware per l'utente root. Di conseguenza, un dispositivo MFA virtuale potrebbe non offrire lo stesso livello di sicurezza di un dispositivo hardware MFA. È possibile utilizzare l'MFA virtuale in attesa dell'approvazione o della consegna dell'acquisto dell'hardware.

In situazioni in cui si gestiscono centinaia di account AWS Organizations, a seconda della propensione al rischio dell'organizzazione, potrebbe non essere scalabile utilizzare la MFA basata su hardware per l'utente root di ogni account in un'unità organizzativa (OU). In questo caso, è

possibile scegliere un account nell'unità organizzativa che funga da account di gestione dell'unità organizzativa e quindi disabilitare l'utente root per gli altri account dell'unità organizzativa. Per impostazione predefinita, l'account di gestione dell'unità organizzativa non ha accesso agli altri account. Configurando in anticipo l'accesso tra più account, è possibile accedere agli altri account dall'account di gestione dell'unità organizzativa in caso di emergenza. Per configurare l'accesso tra più account, si crea un ruolo IAM nell'account membro e si definiscono le politiche in modo che solo l'utente root dell'account di gestione dell'unità organizzativa possa assumere questo ruolo. Per ulteriori informazioni, consulta Tutorial: Delegate l'accesso attraverso l' Account AWS utilizzo dei ruoli IAM nella documentazione IAM.

Ti consigliamo di abilitare più dispositivi MFA per le credenziali dell'utente root. È possibile registrare fino a otto dispositivi MFA di qualsiasi combinazione.

Per maggiori informazioni, consulta le seguenti risorse:

- Abilitazione di un token TOTP hardware nella documentazione IAM
- Abilitazione di un dispositivo di autenticazione a più fattori (MFA) virtuale nella documentazione IAM
- Abilitazione di una chiave di sicurezza FIDO nella documentazione IAM
- Proteggi l'accesso dell'utente root con l'autenticazione a più fattori (MFA) nella documentazione IAM

Segui le best practice di sicurezza per IAM

La documentazione IAM include un elenco di best practice progettate per aiutarti a proteggere Account AWS le tue risorse. Include raccomandazioni per configurare l'accesso e le autorizzazioni in base al principio del privilegio minimo. Esempi di best practice di sicurezza IAM includono la configurazione della federazione delle identità, la richiesta della MFA e l'utilizzo di credenziali temporanee.

Per maggiori informazioni, consulta le seguenti risorse:

- Le migliori pratiche di sicurezza in IAM nella documentazione IAM
- Utilizzo di credenziali temporanee con AWS risorse nella documentazione IAM

Concedi le autorizzazioni con il privilegio minimo

Il privilegio minimo è la pratica di concedere solo le autorizzazioni necessarie per eseguire un'attività. A tale scopo, è necessario definire le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche.

Il controllo degli accessi basato sugli attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, come i relativi tag. È possibile utilizzare gli attributi di gruppo, identità e risorsa per definire dinamicamente le autorizzazioni su larga scala, anziché definire le autorizzazioni per singoli utenti. Ad esempio, puoi utilizzare ABAC per consentire a un gruppo di sviluppatori di accedere solo alle risorse a cui è associato un tag specifico al progetto.

Per maggiori informazioni, consulta le seguenti risorse:

- Applica le autorizzazioni con privilegi minimi nella documentazione IAM
- A cosa serve ABAC nella documentazione IAM AWS

Definisci le barriere di autorizzazione a livello di carico di lavoro

È consigliabile utilizzare una strategia multi-account perché offre la flessibilità necessaria per definire i guardrail a livello di carico di lavoro. La AWS Security Reference Architecture offre indicazioni prescrittive su come strutturare gli account. Questi account vengono gestiti come organizzazione in AWS Organizations, e gli account sono raggruppati in unità organizzative (). OUs

Servizi AWS, ad esempio AWS Control Tower, può aiutarti a gestire centralmente i controlli all'interno di un'organizzazione. Ti consigliamo di definire uno scopo chiaro per ogni account o unità organizzativa all'interno dell'organizzazione e di applicare i controlli in base a tale scopo. AWS Control Tower implementa controlli preventivi, investigativi e proattivi che consentono di gestire le risorse e monitorare la conformità. Un controllo preventivo è progettato per prevenire il verificarsi di un evento. Un controllo investigativo è progettato per rilevare, registrare e avvisare dopo che si è verificato un evento. Un controllo proattivo è progettato per impedire l'implementazione di risorse non conformi mediante la scansione delle risorse prima del loro approvvigionamento.

Per maggiori informazioni, consulta le seguenti risorse:

- Separare i carichi di lavoro utilizzando gli account nel AWS Well-Architected Framework
- AWS Architettura di riferimento per la sicurezza (AWS SRA) nelle linee guida prescrittive AWS

- Informazioni sui controlli presenti nella documentazione AWS Control Tower AWS Control Tower
- Implementazione dei controlli di sicurezza AWS in AWS Prescriptive Guidance
- Utilizza le politiche di controllo dei servizi per impostare barriere di autorizzazione tra gli account della tua AWS organizzazione nel Security Blog AWS

Ruota le chiavi di accesso IAM a intervalli regolari

È consigliabile aggiornare le chiavi di accesso per i casi d'uso che richiedono credenziali a lungo termine. Consigliamo di ruotare le chiavi di accesso ogni 90 giorni o meno. La rotazione delle chiavi di accesso riduce il rischio che venga utilizzata una chiave di accesso associata a un account compromesso o chiuso. Inoltre, impedisce l'accesso utilizzando una vecchia chiave che potrebbe essere stata smarrita, compromessa o rubata. Aggiorna sempre le applicazioni dopo aver ruotato le chiavi di accesso.

Per maggiori informazioni, consulta le seguenti risorse:

- Aggiorna le chiavi di accesso quando necessario per i casi d'uso che richiedono credenziali a lungo termine nella documentazione IAM
- Ruota automaticamente le chiavi di accesso utente IAM su larga scala con AWS Organizations e Gestione dei segreti AWS in AWS Prescriptive Guidance
- Aggiornamento delle chiavi di accesso nella documentazione IAM

Identifica le risorse condivise con un'entità esterna

Un'entità esterna è una risorsa, un'applicazione, un servizio o un utente esterno all' AWS organizzazione, ad esempio un altro utente root Account AWS, un utente o ruolo IAM, un utente federato o un Servizio AWS utente anonimo (o non autenticato). È una best practice di sicurezza utilizzare IAM Access Analyzer per identificare le risorse dell'organizzazione e degli account, come i bucket Amazon Simple Storage Service (Amazon S3) o i ruoli IAM, che sono condivisi con un'entità esterna. Questo ti aiuta a identificare l'accesso involontario a risorse e dati, che rappresenta un rischio per la sicurezza.

Per maggiori informazioni, consulta le seguenti risorse:

- Verifica l'accesso pubblico e tra account alle risorse con IAM Access Analyzer nella documentazione IAM

- Analizza l'accesso pubblico e tra account nel AWS Well-Architected Framework
- Utilizzo AWS Identity and Access Management Access Analyzer nella documentazione IAM

Raccomandazioni sul controllo di sicurezza per la registrazione e il monitoraggio

La registrazione e il monitoraggio sono aspetti importanti del rilevamento delle minacce. Il rilevamento delle minacce è una delle funzionalità dal punto di vista della sicurezza del AWS Cloud Adoption Framework (AWS CAF). Utilizzando i dati di registro, l'organizzazione può monitorare l'ambiente per comprendere e identificare potenziali errori di configurazione della sicurezza, minacce e comportamenti imprevisti. La comprensione delle potenziali minacce può aiutare l'organizzazione a dare priorità ai controlli di sicurezza e un rilevamento efficace delle minacce può aiutare a rispondere alle minacce più rapidamente.

Controlli in questa sezione:

- Configura almeno un percorso multiregionale in CloudTrail
- Configurare la registrazione a livello di servizio e applicazione
- Stabilisci una posizione centralizzata per analizzare i log e rispondere agli eventi di sicurezza
- Impedisci l'accesso non autorizzato ai bucket S3 che contengono file di registro CloudTrail
- Configura gli avvisi per le modifiche ai gruppi di sicurezza o alla rete ACLs
- Configura gli avvisi per gli CloudWatch allarmi che entrano nello stato ALARM

Configura almeno un percorso multiregionale in CloudTrail

AWS CloudTrailti aiuta a verificare la governance, la conformità e il rischio operativo del tuo Account AWS. Le azioni intraprese da un utente, un ruolo o un utente Servizio AWS vengono registrate come eventi in CloudTrail. Gli eventi includono le azioni intraprese in Console di gestione AWS, AWS Command Line Interface (AWS CLI) e AWS SDKs e APIs. Questa cronologia degli eventi consente di analizzare il livello di sicurezza, tenere traccia delle modifiche alle risorse e verificare la conformità.

Per una registrazione continua degli eventi della tua azienda Account AWS, devi creare un percorso. Ogni percorso deve essere configurato per registrare tutti gli eventi Regioni AWS. Registrando tutti gli eventi Regioni AWS, ti assicuri che tutti gli eventi che si verificano nel tuo Account AWS vengano registrati, indipendentemente dal luogo in cui si Regione AWS sono verificati. Un percorso multiregionale garantisce la registrazione degli eventi di servizio globali.

Per maggiori informazioni, consulta le seguenti risorse:

- CloudTrail le migliori pratiche di sicurezza per gli investigatori contenute nella documentazione CloudTrail
- Conversione di un percorso che si applica a una regione in modo da applicarlo a tutte le regioni della documentazione CloudTrail
- Abilitazione e disabilitazione della registrazione degli eventi di servizio globale nella documentazione CloudTrail

Configurare la registrazione a livello di servizio e applicazione

AWS Well-Architected Framework consiglia di conservare i registri degli eventi di sicurezza di servizi e applicazioni. Si tratta di un principio fondamentale di sicurezza per audit, indagini e casi d'uso operativi. La conservazione dei log dei servizi e delle applicazioni è un requisito di sicurezza comune, determinato dagli standard, dalle politiche e dalle procedure di governance, rischio e conformità (GRC).

I team addetti alle operazioni di sicurezza si affidano ai log e agli strumenti di ricerca per scoprire potenziali eventi di interesse che potrebbero indicare attività non autorizzate o modifiche involontarie. È possibile abilitare la registrazione per diversi servizi, a seconda del caso d'uso. Ad esempio, puoi registrare l'accesso al bucket Amazon S3, il traffico AWS WAF Web ACL, il traffico Amazon API Gateway a livello di rete o le distribuzioni Amazon. CloudFront

Per maggiori informazioni, consulta le seguenti risorse:

- Trasmetti Amazon CloudWatch Logs a un account centralizzato per il controllo e l'analisi nel blog di architettura AWS
- Configurare la registrazione di servizi e applicazioni nel AWS Well-Architected Framework

Stabilisci una posizione centralizzata per analizzare i log e rispondere agli eventi di sicurezza

L'analisi manuale dei log e l'elaborazione delle informazioni non sono sufficienti per tenere il passo con il volume di informazioni associato alle architetture complesse. L'analisi e il reporting da soli non facilitano l'assegnazione tempestiva degli eventi alla risorsa corretta. Il AWS Well-Architected Framework consiglia di AWS integrare gli eventi e i risultati di sicurezza in un sistema di notifica e flusso di lavoro, ad esempio un sistema di ticketing, bug o di gestione delle informazioni e degli

eventi di sicurezza (SIEM). Questi sistemi consentono di assegnare, indirizzare e gestire gli eventi di sicurezza.

Per maggiori informazioni, consulta le seguenti risorse:

- Analizza log, risultati e metriche centralmente nel Well-Architected Framework AWS
- Analizza la sicurezza, la conformità e l'attività operativa utilizzando CloudTrail Amazon Athena nel blog sulla AWS sicurezza
- AWS Partner che forniscono servizi di rilevamento e risposta alle minacce nel AWS Partners Portfolio

Impedisci l'accesso non autorizzato ai bucket S3 che contengono file di registro CloudTrail

Per impostazione predefinita, i file di CloudTrail log vengono archiviati in bucket Amazon S3. È una best practice di sicurezza quella di impedire l'accesso non autorizzato a qualsiasi bucket Amazon S3 che CloudTrail contiene file di registro. Questo ti aiuta a mantenere l'integrità, la completezza e la disponibilità di questi log, il che è fondamentale per scopi forensi e di controllo. Se desideri registrare gli eventi relativi ai dati per i bucket S3 che contengono file di CloudTrail registro, puoi creare un percorso a questo scopo. CloudTrail

Per maggiori informazioni, consulta le seguenti risorse:

- Configurazione delle impostazioni di accesso pubblico a blocchi per i bucket S3 nella documentazione di Amazon S3
- CloudTrail le migliori pratiche di sicurezza preventiva nella documentazione CloudTrail
- Creazione di una traccia nella documentazione CloudTrail

Configura gli avvisi per le modifiche ai gruppi di sicurezza o alla rete ACLs

Un gruppo di sicurezza in Amazon Virtual Private Cloud (Amazon VPC) controlla il traffico a cui è consentito raggiungere e uscire dalle risorse a cui è associato. Una lista di controllo degli accessi alla rete (ACL) consente o nega traffico specifico in entrata o in uscita a livello di sottorete del VPC. Queste risorse sono fondamentali per la gestione dell'accesso nel tuo ambiente. AWS

Crea e configura un CloudWatch allarme Amazon che ti avvisi in caso di modifiche alla configurazione di un gruppo di sicurezza o di un ACL di rete. Configura questo allarme per avvisarti ogni volta che viene eseguita una chiamata AWS API per aggiornare i gruppi di sicurezza. Puoi anche utilizzare servizi, come Amazon EventBridge e AWS Config, per rispondere automaticamente a questi tipi di eventi di sicurezza.

Per maggiori informazioni, consulta le seguenti risorse:

- Ripristina e ricevi automaticamente notifiche sulle modifiche ai tuoi gruppi di sicurezza Amazon VPC nel AWS Security Blog
- Utilizzo degli CloudWatch allarmi Amazon nella documentazione CloudWatch
- Implementa eventi di sicurezza utilizzabili nel Well-Architected AWS Framework
- Automatizza la risposta agli eventi nel AWS Well-Architected Framework

Configura gli avvisi per gli CloudWatch allarmi che entrano nello stato ALARM

In CloudWatch, è possibile specificare le azioni intraprese da un allarme quando cambia stato tra gli stati `OKALARM`, e`INSUFFICIENT_DATA`. Il tipo più comune di azione di allarme consiste nell'avvisare una o più persone inviando un messaggio a un argomento di Amazon Simple Notification Service (Amazon SNS). Puoi anche configurare allarmi da creare OpsItemso attivare incidenti. AWS Systems Manager

Ti consigliamo di attivare le azioni di allarme per avvisare automaticamente se una metrica monitorata non rientra nella soglia definita. Il monitoraggio degli allarmi consente di identificare attività insolite e di rispondere rapidamente ai problemi operativi e di sicurezza.

Per maggiori informazioni, consulta le seguenti risorse:

- Implementa eventi di sicurezza utilizzabili nel Well-Architected AWS Framework
- Azioni di allarme nella documentazione CloudWatch

Raccomandazioni sul controllo della sicurezza per proteggere l'infrastruttura

La protezione dell'infrastruttura è una parte fondamentale di qualsiasi programma di sicurezza. Include metodologie di controllo che aiutano a proteggere le reti e le risorse di elaborazione. Esempi di protezione dell'infrastruttura includono i limiti di fiducia, un defense-in-depth approccio, il rafforzamento della sicurezza, la gestione delle patch e l'autenticazione e l'autorizzazione del sistema operativo. Per ulteriori informazioni, vedere Protezione dell'infrastruttura nel AWS Well-Architected Framework. I controlli di sicurezza in questa sezione possono aiutarti a implementare le migliori pratiche per la protezione dell'infrastruttura.

Controlli in questa sezione:

- Specificare gli oggetti radice predefiniti per le CloudFront distribuzioni
- Scansiona il codice dell'applicazione per identificare i problemi di sicurezza più comuni
- Crea livelli di rete utilizzando sottoreti e sottoreti dedicate VPCs
- Limita il traffico in entrata solo alle porte autorizzate
- Blocca l'accesso pubblico ai documenti di Systems Manager
- Blocca l'accesso pubblico alle funzioni Lambda
- Limita il traffico in entrata e in uscita nel gruppo di sicurezza predefinito
- Scansiona le vulnerabilità del software e l'esposizione involontaria della rete
- Configurare AWS WAF
- Configura protezioni avanzate contro gli attacchi S DDo
- Utilizza un defense-in-depth approccio per controllare il traffico di rete

Specificare gli oggetti radice predefiniti per le CloudFront distribuzioni

Amazon CloudFront accelera la distribuzione dei tuoi contenuti web distribuendoli attraverso una rete mondiale di data center, che riduce la latenza e migliora le prestazioni. Se non definisci un oggetto root predefinito, le richieste per il percorso root della distribuzione passa al tuo server di origine. Se utilizzi un'origine Amazon Simple Storage Service (Amazon S3), la richiesta potrebbe restituire un

elenco dei contenuti nel tuo bucket S3 o un elenco dei contenuti privati della tua origine. Specificare un oggetto root predefinito ti aiuta a evitare di esporre il contenuto della tua distribuzione.

Per maggiori informazioni, consulta le seguenti risorse:

- Specificare un oggetto radice predefinito nella documentazione CloudFront

Scansiona il codice dell'applicazione per identificare i problemi di sicurezza più comuni

Il AWS Well-Architected Framework consiglia di scansionare le librerie e le dipendenze per individuare problemi e difetti. Esistono molti strumenti di analisi del codice sorgente che è possibile utilizzare per eseguire la scansione del codice sorgente. Ad esempio, Amazon CodeGuru può analizzare i problemi di sicurezza più comuni nelle Java nostre Python applicazioni e fornire consigli per risolverli.

Per maggiori informazioni, consulta le seguenti risorse:

- CodeGuru documentazione
- strumenti di analisi del codice sorgente sul OWASP Foundation sito web
- Esegui la gestione delle vulnerabilità nel AWS Well-Architected Framework

Crea livelli di rete utilizzando sottoreti e sottoreti dedicate VPCs

Il AWS Well-Architected Framework consiglia di raggruppare i componenti che condividono i requisiti di sensibilità in livelli. Ciò riduce al minimo il potenziale ambito di impatto dell'accesso non autorizzato. Ad esempio, un cluster di database che non richiede l'accesso a Internet deve essere collocato in una sottorete privata del suo VPC per assicurarsi che non vi sia alcun percorso da o verso Internet.

AWS offre molti servizi che possono aiutarti a testare e identificare la raggiungibilità pubblica. Ad esempio, Reachability Analyzer è uno strumento di analisi della configurazione che consente di testare la connettività tra le risorse di origine e di destinazione nel proprio. VPCs Inoltre, Network Access Analyzer può aiutarvi a identificare accessi involontari di rete alle risorse.

Per maggiori informazioni, consulta le seguenti risorse:

- Crea livelli di rete nel AWS Well-Architected Framework
- Documentazione Reachability Analyzer
- Documentazione di Network Access Analyzer
- Crea una sottorete nella documentazione di Amazon Virtual Private Cloud (Amazon VPC)

Limita il traffico in entrata solo alle porte autorizzate

L'accesso illimitato, ad esempio il traffico proveniente dall'indirizzo IP di `0.0.0.0/0` origine, aumenta il rischio di attività dannose, come pirateria informatica, attacchi (denial-of-serviceDoS) e perdita di dati. I gruppi di sicurezza forniscono un filtraggio statico del traffico di rete in ingresso e in uscita verso le risorse. AWS Nessun gruppo di sicurezza dovrebbe consentire l'accesso illimitato in ingresso a porte note, come SSH e RDP (Remote Desktop Protocol). Windows Per il traffico in entrata, nei tuoi gruppi di sicurezza, consenti solo le connessioni TCP o UDP sulle porte autorizzate. Per connetterti alle istanze Amazon Elastic Compute Cloud (Amazon EC2), usa Session Manager o Run Command anziché l'accesso diretto SSH o RDP.

Per maggiori informazioni, consulta le seguenti risorse:

- Lavora con i gruppi di sicurezza nella documentazione di Amazon EC2
- Controlla il traffico verso AWS le tue risorse utilizzando i gruppi di sicurezza nella documentazione di Amazon VPC

Blocca l'accesso pubblico ai documenti di Systems Manager

A meno che il caso d'uso non richieda l'attivazione della condivisione pubblica, le AWS Systems Manager best practice consigliano di bloccare la condivisione pubblica per i documenti di Systems Manager. La condivisione pubblica potrebbe consentire l'accesso non intenzionale ai documenti. Un documento pubblico di Systems Manager può esporre informazioni preziose e sensibili sull'account, sulle risorse e sui processi interni.

Per maggiori informazioni, consulta le seguenti risorse:

- Procedure ottimali per i documenti condivisi di Systems Manager nella documentazione di Systems Manager
- Modifica le autorizzazioni per un documento Systems Manager condiviso nella documentazione di Systems Manager

Blocca l'accesso pubblico alle funzioni Lambda

AWS Lambda è un servizio di calcolo che consente di eseguire il codice senza gestire i server o effettuarne il provisioning. Le funzioni Lambda non dovrebbero essere accessibili pubblicamente perché ciò potrebbe consentire l'accesso involontario al codice della funzione.

Ti consigliamo di configurare politiche basate sulle risorse per le funzioni Lambda per negare l'accesso dall'esterno del tuo account. È possibile ottenere ciò rimuovendo le autorizzazioni o aggiungendo la `AWS:SourceAccount` condizione all'istruzione che consente l'accesso. Puoi aggiornare le politiche basate sulle risorse per le funzioni Lambda tramite l'API Lambda o (). AWS Command Line Interface AWS CLI

Ti consigliamo inoltre di abilitare la funzione [Lambda.1] Le politiche della funzione Lambda dovrebbero vietare il controllo dell'accesso pubblico in. AWS Security Hub CSPM Questo controllo verifica che le politiche basate sulle risorse per le funzioni Lambda vietino l'accesso pubblico.

Per maggiori informazioni, consulta le seguenti risorse:

- AWS Lambda controlli nella documentazione CSPM di Security Hub
- Utilizzo di politiche basate sulle risorse per Lambda nella documentazione di Lambda
- Risorse e condizioni per le azioni Lambda nella documentazione Lambda

Limita il traffico in entrata e in uscita nel gruppo di sicurezza predefinito

Se non associ un gruppo di sicurezza personalizzato quando esegui il provisioning di una AWS risorsa, la risorsa viene associata al gruppo di sicurezza predefinito del VPC. Le regole predefinite per questo gruppo di sicurezza consentono tutto il traffico in entrata da tutte le risorse assegnate a questo gruppo di sicurezza e consentono tutto il traffico in uscita e in uscita IPv4 . IPv6 Ciò potrebbe consentire il traffico involontario verso la risorsa.

AWS consiglia di non utilizzare il gruppo di sicurezza predefinito. Crea invece gruppi di sicurezza personalizzati per risorse o gruppi di risorse specifici.

Poiché il gruppo di sicurezza predefinito non può essere eliminato, ti consigliamo di modificare le regole del gruppo di sicurezza predefinito per limitare il traffico in entrata e in uscita. Quando configuri le regole del gruppo di sicurezza, segui il principio del privilegio minimo.

Ti consigliamo inoltre di abilitare il [EC2.2] VPC predefinito. I gruppi di sicurezza non dovrebbero consentire il controllo del traffico in entrata o in uscita in Security Hub CSPM. Questo controllo verifica che il gruppo di sicurezza predefinito di un VPC neghi il traffico in entrata e in uscita.

Per maggiori informazioni, consulta le seguenti risorse:

- Controlla il traffico verso AWS le tue risorse utilizzando i gruppi di sicurezza nella documentazione di Amazon VPC
- Gruppi di sicurezza predefiniti per te VPCs nella documentazione di Amazon VPC
- Controlli di Amazon EC2 nella documentazione CSPM di Security Hub

Scansiona le vulnerabilità del software e l'esposizione involontaria della rete

Ti consigliamo di abilitare Amazon Inspector in tutti i tuoi account. Amazon Inspector è un servizio di gestione delle vulnerabilità che analizza continuamente le istanze Amazon EC2, le immagini dei container Amazon Elastic Container Registry (Amazon ECR) e le funzioni Lambda alla ricerca di vulnerabilità del software ed esposizione involontaria alla rete. Supporta anche l'ispezione approfondita delle istanze Amazon EC2. Quando Amazon Inspector identifica una vulnerabilità o un percorso di rete aperto, produce un risultato che puoi esaminare. Se Amazon Inspector e Security Hub CSPM sono entrambi configurati nel tuo account, Amazon Inspector invia automaticamente i risultati di sicurezza a Security Hub CSPM per la gestione centralizzata.

Per maggiori informazioni, consulta le seguenti risorse:

- Scansione delle risorse con Amazon Inspector nella documentazione di Amazon Inspector
- Amazon Inspector Ispezione approfondita per Amazon EC2 nella documentazione di Amazon Inspector
- Scansiona EC2 AMIs utilizzando Amazon Inspector nel AWS blog sulla sicurezza
- Creazione di un programma scalabile di gestione delle vulnerabilità su Prescriptive Guidance AWS AWS
- Automatizza la protezione della rete nel AWS Well-Architected Framework
- Automatizza la protezione dell'elaborazione nel Well-Architected AWS Framework

Configurare AWS WAF

AWS WAFè un firewall per applicazioni Web che consente di monitorare e bloccare le richieste HTTP o HTTPS inoltrate alle risorse protette delle applicazioni Web, come Amazon API Gateway, CloudFront distribuzioni APIs Amazon o Application Load Balancers. In base ai criteri specificati, il servizio risponde alle richieste con il contenuto richiesto, con un codice di stato HTTP 403 (Forbidden) o con una risposta personalizzata. AWS WAF può aiutare a proteggere le applicazioni Web o APIs da exploit Web comuni che possono influire sulla disponibilità, compromettere la sicurezza o consumare risorse eccessive. Prendi AWS WAF in considerazione la possibilità di configurarla internamente Account AWS e di utilizzare una combinazione di regole AWS gestite, regole personalizzate e integrazioni con i partner per proteggere le applicazioni dagli attacchi a livello applicativo (livello 7).

Per maggiori informazioni, consulta le seguenti risorse:

- Guida introduttiva AWS WAF alla documentazione AWS WAF
- AWS WAF partner di consegna sul AWS sito web
- Automazioni di sicurezza per AWS WAF nella AWS Solutions Library
- Implementa l'ispezione e la protezione nel AWS Well-Architected Framework

Configura protezioni avanzate contro gli attacchi S DDo

AWS Shieldfornisce protezioni contro gli attacchi Distributed Denial of Service (DDoS) per AWS le risorse a livello di rete e trasporto (livello 3 e 4) e a livello di applicazione (livello 7). Questo servizio è disponibile in due opzioni: AWS Shield Standard e. AWS Shield Advanced Shield Standard protegge automaticamente AWS le risorse supportate, senza costi aggiuntivi.

Ti consigliamo di abbonarti a Shield Advanced, che offre una protezione estesa dagli attacchi DDo S per le risorse protette. Le protezioni che ricevi da Shield Advanced variano a seconda dell'architettura e delle scelte di configurazione. Prendi in considerazione l'implementazione delle protezioni Shield Advanced per le applicazioni in cui è necessario uno dei seguenti elementi:

- Disponibilità garantita per gli utenti dell'applicazione.
- Accesso rapido agli esperti di mitigazione DDo S se l'applicazione è interessata da un attacco DDo S.

- Consapevolezza da parte di AWS del fatto che l'applicazione potrebbe essere interessata da un attacco DDo S e notifica degli attacchi da parte di AWS e segnalazione ai team di sicurezza o operativi.
- La prevedibilità dei costi del cloud, anche quando un attacco DDo S influisce sull'utilizzo di. Servizi AWS

Per maggiori informazioni, consulta le seguenti risorse:

- AWS Shield Advanced panoramica nella documentazione di Shield
- AWS Shield Advanced risorse protette nella documentazione di Shield
- AWS Shield Advanced funzionalità e opzioni nella documentazione di Shield
- Risposta agli eventi DDo S nella documentazione di Shield
- Implementa l'ispezione e la protezione nel AWS Well-Architected Framework

Utilizza un defense-in-depth approccio per controllare il traffico di rete

AWS Network Firewall è un firewall di rete a stato gestito e un servizio di rilevamento e prevenzione delle intrusioni per cloud privati virtuali (VPCs) in. Cloud AWS Ti aiuta a implementare le protezioni di rete essenziali lungo il perimetro del VPC. Ciò include il filtraggio del traffico in entrata e in arrivo da un gateway Internet, un gateway NAT o tramite VPN o. AWS Direct Connect Network Firewall include funzionalità che aiutano a proteggere dalle minacce di rete più comuni. Il firewall stateful di Network Firewall può incorporare il contesto dei flussi di traffico, come connessioni e protocolli, per applicare le politiche.

Per maggiori informazioni, consulta le seguenti risorse:

- AWS Network Firewall documentazione
- Controlla il traffico a tutti i livelli nel AWS Well-Architected Framework

Raccomandazioni sul controllo di sicurezza per proteggere i dati

Il AWS Well-Architected Framework raggruppa le migliori pratiche per la protezione dei dati in tre categorie: classificazione dei dati, protezione dei dati inattivi e protezione dei dati in transito. I controlli di sicurezza in questa sezione possono aiutarti a implementare le migliori pratiche per la protezione dei dati. Queste best practice fondamentali devono essere implementate prima di progettare qualsiasi carico di lavoro nel cloud. Impediscono la cattiva gestione dei dati e aiutano a soddisfare gli obblighi organizzativi, normativi e di conformità. Utilizza i controlli di sicurezza in questa sezione per implementare le migliori pratiche per la protezione dei dati.

Controlli in questa sezione:

- Identifica e classifica i dati a livello di carico di lavoro
- Stabilisci controlli per ogni livello di classificazione dei dati
- Crittografa i dati inattivi
- Crittografa i dati in transito
- Blocca l'accesso pubblico agli snapshot di Amazon EBS
- Blocca l'accesso pubblico agli snapshot di Amazon RDS
- Blocca l'accesso pubblico ad Amazon RDS, Amazon Redshift e alle risorse AWS DMS
- Blocca l'accesso pubblico ai bucket Amazon S3
- Richiedi l'autenticazione a più fattori per eliminare i dati nei bucket Amazon S3 critici
- Configura i domini Amazon OpenSearch Service in un VPC
- Configura gli avvisi per l'eliminazione AWS KMS key
- Blocca l'accesso pubblico a AWS KMS keys
- Configura i listener di load balancer per utilizzare protocolli sicuri

Identifica e classifica i dati a livello di carico di lavoro

La classificazione dei dati è 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 spesso riduce la frequenza della duplicazione dei dati. Ciò può ridurre i costi di archiviazione e backup e accelerare le ricerche.

Ti consigliamo di comprendere il tipo e la classificazione dei dati che il tuo carico di lavoro sta elaborando, i processi aziendali associati, dove vengono archiviati i dati e chi è il proprietario dei dati. La classificazione dei dati aiuta i proprietari dei carichi di lavoro a identificare le ubicazioni in cui sono archiviati i dati sensibili e a determinare in che modo accedere e condividere tali dati. I tag sono coppie chiave-valore che fungono da metadati per l'organizzazione delle risorse. AWS I tag possono aiutare a gestire, identificare, organizzare, cercare e filtrare le risorse.

Per maggiori informazioni, consulta le seguenti risorse:

- Classificazione dei dati nei AWS white paper
- Identifica i dati all'interno del tuo carico di lavoro nel AWS Well-Architected Framework

Stabilisci controlli per ogni livello di classificazione dei dati

Definisci i controlli di protezione dei dati per ogni livello di classificazione. Ad esempio, utilizza i controlli consigliati per proteggere i dati classificati come pubblici e proteggere i dati sensibili con controlli aggiuntivi. Utilizza meccanismi e strumenti che riducano o eliminino la necessità di accedere direttamente ai dati o di elaborarli manualmente. L'automazione dell'identificazione e della classificazione dei dati riduce il rischio di errori di classificazione, gestione, modifica o errore umano.

Ad esempio, prendi in considerazione l'utilizzo di Amazon Macie per scansionare i bucket Amazon Simple Storage Service (Amazon S3) alla ricerca di dati sensibili, come informazioni di identificazione personale (PII). Inoltre, puoi automatizzare il rilevamento di accessi non intenzionali ai dati utilizzando VPC Flow Logs in Amazon Virtual Private Cloud (Amazon VPC).

Per maggiori informazioni, consulta le seguenti risorse:

- Definisci i controlli di protezione dei dati nel AWS Well-Architected Framework
- Automatizza l'identificazione e la classificazione nel AWS Well-Architected Framework
- AWS Architettura di riferimento per la privacy (AWS PRA) nelle linee guida prescrittive AWS
- Alla scoperta di dati sensibili con Amazon Macie nella documentazione di Macie
- Registrazione del traffico IP tramite VPC Flow Logs nella documentazione di Amazon VPC
- Tecniche comuni per rilevare dati PHI e PII utilizzate nel blog di for Industries Servizi AWS AWS

Crittografa i dati inattivi

I dati inattivi sono dati fissi nella rete, ad esempio i dati archiviati. L'implementazione della crittografia e dei controlli di accesso appropriati per i dati archiviati aiuta a ridurre il rischio di accesso non autorizzato. La crittografia è un processo informatico che trasforma i dati in chiaro, leggibili dall'uomo, in testo cifrato. È necessaria una chiave di crittografia per decrittografare il contenuto in testo semplice in modo che possa essere utilizzato. In Cloud AWS, puoi usare AWS Key Management Service (AWS KMS) per creare e controllare chiavi crittografiche che aiutano a proteggere i tuoi dati.

Come discusso in precedenzaStabilisci controlli per ogni livello di classificazione dei dati, consigliamo di creare una politica che specifichi il tipo di dati che richiede la crittografia. Includi criteri su come determinare quali dati devono essere crittografati e quali dati devono essere protetti con un'altra tecnica, come la tokenizzazione o l'hashing.

Per maggiori informazioni, consulta le seguenti risorse:

- Configurazione della crittografia predefinita nella documentazione di Amazon S3
- Crittografia predefinita per nuovi volumi EBS e copie di snapshot nella documentazione di Amazon EC2
- Crittografia delle risorse Amazon Aurora nella documentazione di Amazon Aurora
- Introduzione ai dettagli crittografici contenuti nella documentazione AWS KMS AWS KMS
- Creazione di una strategia di crittografia aziendale per i dati inattivi in AWS Prescriptive Guidance
- Applica la crittografia a riposo nel AWS Well-Architected Framework
- Per ulteriori informazioni specifiche sulla crittografia Servizi AWS, consulta la AWS documentazione relativa al servizio

Crittografa i dati in transito

I dati in transito sono dati che si spostano attivamente attraverso la rete, ad esempio tra le risorse di rete. Crittografa tutti i dati in transito utilizzando protocolli TLS sicuri e suite di crittografia. Il traffico di rete tra le risorse e Internet deve essere crittografato per impedire l'accesso non autorizzato ai dati. Quando possibile, utilizzate TLS per crittografare il traffico di rete all'interno del vostro ambiente interno. AWS

Per maggiori informazioni, consulta le seguenti risorse:

- Richiesta di HTTPS per la comunicazione tra gli spettatori e CloudFront nella documentazione di Amazon CloudFront
- Documentazione di AWS PrivateLink
- Applica la crittografia in transito nel AWS Well-Architected Framework
- Per ulteriori informazioni specifiche sulla crittografia Servizi AWS, consulta la AWS documentazione relativa a quel servizio

Blocca l'accesso pubblico agli snapshot di Amazon EBS

Amazon Elastic Block Store (Amazon EBS) fornisce volumi di storage a livello di blocco da utilizzare con le istanze Amazon Elastic Compute Cloud (Amazon EC2). Puoi eseguire il backup dei dati sui tuoi volumi Amazon EBS su Amazon S3 scattando point-in-time istantanee. Puoi condividere le istantanee pubblicamente con tutti gli altri Account AWS oppure puoi condividerle privatamente con una persona da te specificata. Account AWS

Ti consigliamo di non condividere pubblicamente le istantanee di Amazon EBS. Ciò potrebbe esporre inavvertitamente dati sensibili. Quando condividi un'istantanea, consenti ad altri di accedere ai dati in essa contenuti. Condividi le istantanee solo con persone di cui ti fidi e che dispongono di tutti questi dati.

Per maggiori informazioni, consulta le seguenti risorse:

- Condividi uno snapshot nella documentazione di Amazon EC2
- Gli snapshot di Amazon EBS non devono essere ripristinabili pubblicamente nella documentazione AWS Security Hub CSPM
- ebs-snapshot-public-restorable-controlla la documentazione AWS Config

Blocca l'accesso pubblico agli snapshot di Amazon RDS

Amazon Relational Database Service (Amazon RDS) ti aiuta a configurare, gestire e scalare un database relazionale in. Cloud AWS Amazon RDS crea e salva backup automatici dell'istanza di database (DB) o del cluster DB Multi-AZ durante la finestra di backup dell'istanza DB. Amazon RDS crea uno snapshot dei volumi di storage dell'istanza database, eseguendo il backup dell'intera istanza database anziché dei singoli database. Puoi condividere uno snapshot manuale allo scopo di copiarlo o ripristinare un'istanza DB da esso.

Se condividi un'istantanea come pubblica, assicurati che nessuno dei dati in essa contenuti sia privato o sensibile. Quando un'istantanea viene condivisa pubblicamente, concede a tutti i Account AWS permessi per accedere ai dati. Ciò può comportare un'esposizione involontaria dei dati nella tua istanza Amazon RDS.

Per maggiori informazioni, consulta le seguenti risorse:

- Condivisione di uno snapshot DB nella documentazione di Amazon RDS
- rds-snapshots-public-prohibitednella documentazione AWS Config
- L'istantanea RDS deve essere privata nella documentazione CSPM di Security Hub

Blocca l'accesso pubblico ad Amazon RDS, Amazon Redshift e alle risorse AWS DMS

Puoi configurare le istanze DB di Amazon RDS, i cluster Amazon Redshift AWS Database Migration Service e le istanze di replica AWS DMS() in modo che siano accessibili al pubblico. Se il valore del `publiclyAccessible` campo è`true`, queste risorse sono accessibili pubblicamente. Consentire l'accesso pubblico può comportare traffico, esposizione o fughe di dati non necessari. Ti consigliamo di non consentire l'accesso pubblico a queste risorse.

Ti consigliamo di abilitare AWS Config le regole o i controlli CSPM di Security Hub per rilevare se le istanze DB di Amazon RDS, le istanze di AWS DMS replica o i cluster Amazon Redshift consentono l'accesso pubblico.

> **Note**
>
> Le impostazioni di accesso pubblico per le istanze di AWS DMS replica non possono essere modificate dopo il provisioning dell'istanza. Per modificare l'impostazione di accesso pubblico, elimina l'istanza corrente e quindi ricreala. Quando la ricreate, non selezionate l'opzione Accessibile pubblicamente.

Per maggiori informazioni, consulta le seguenti risorse:

- AWS DMS le istanze di replica non devono essere pubbliche nella documentazione CSPM di Security Hub

- Le istanze DB RDS devono vietare l'accesso pubblico nella documentazione del Security Hub (CSPM).
- I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico nella documentazione CSPM di Security Hub
- rds-instance-public-access AWS Config -controlla la documentazione
- dms-replication-not-publicnella documentazione AWS Config
- redshift-cluster-public-access-controlla la documentazione AWS Config
- Modifica di un'istanza database Amazon RDS nella documentazione di Amazon RDS
- Modifica di un cluster nella documentazione di Amazon Redshift

Blocca l'accesso pubblico ai bucket Amazon S3

Garantire che i bucket non siano accessibili al pubblico è una best practice di sicurezza di Amazon S3. A meno che tu non richieda esplicitamente a chiunque su Internet di essere in grado di leggere o scrivere nel tuo bucket, assicurati che il bucket non sia pubblico. Questo aiuta a proteggere l'integrità e la sicurezza dei dati. Puoi utilizzare AWS Config le regole e i controlli CSPM di Security Hub per confermare che i bucket Amazon S3 siano conformi a questa best practice.

Per maggiori informazioni, consulta le seguenti risorse:

- Le migliori pratiche di sicurezza di Amazon S3 nella documentazione di Amazon S3
- L'impostazione S3 Block Public Access deve essere abilitata nella documentazione CSPM di Security Hub
- I bucket S3 dovrebbero vietare l'accesso pubblico in lettura nella documentazione CSPM di Security Hub
- I bucket S3 dovrebbero vietare l'accesso pubblico in scrittura nella documentazione CSPM di Security Hub
- regola s3 nella documentazione bucket-public-read-prohibited AWS Config
- s3- bucket-public-write-prohibited nella documentazione AWS Config

Richiedi l'autenticazione a più fattori per eliminare i dati nei bucket Amazon S3 critici

Quando si utilizza la funzione Controllo delle versioni S3 nei bucket Amazon S3, puoi aggiungere un altro livello di sicurezza configurando un bucket per abilitare l'eliminazione MFA (autenticazione a più fattori). In tal caso, il proprietario del bucket deve includere due tipi di autenticazione in qualsiasi richiesta per eliminare una versione o modificare lo stato della funzione Controllo delle versioni del bucket. Ti consigliamo di abilitare questa funzionalità per i bucket che contengono dati fondamentali per la tua organizzazione. Ciò può impedire l'eliminazione accidentale di bucket e dati.

Per maggiori informazioni, consulta le seguenti risorse:

- Configurazione dell'eliminazione MFA nella documentazione di Amazon S3

Configura i domini Amazon OpenSearch Service in un VPC

Amazon OpenSearch Service è un servizio gestito che ti aiuta a distribuire, gestire e scalare OpenSearch i cluster in. Cloud AWS Amazon OpenSearch Service supporta OpenSearch e software Elasticsearch open source legacy (OSS). I domini Amazon OpenSearch Service distribuiti all'interno di un VPC possono comunicare con le risorse VPC sulla AWS rete privata, senza la necessità di attraversare la rete Internet pubblica. Questa configurazione migliora il livello di sicurezza limitando l'accesso ai dati in transito. Ti consigliamo di non collegare domini Amazon OpenSearch Service a sottoreti pubbliche e che il VPC sia configurato secondo le migliori pratiche.

Per maggiori informazioni, consulta le seguenti risorse:

- Avvio dei domini Amazon OpenSearch Service all'interno di un VPC nella documentazione di Amazon Service OpenSearch
- opensearch-in-vpc-onlynella documentazione AWS Config
- OpenSearchi domini devono essere in un VPC nella documentazione CSPM di Security Hub

Configura gli avvisi per l'eliminazione AWS KMS key

AWS Key Management Service (AWS KMS) le chiavi non possono essere recuperate dopo essere state eliminate. Se una chiave KMS viene eliminata, i dati che sono ancora crittografati con quella chiave sono definitivamente irrecuperabili. Se è necessario mantenere l'accesso ai dati, prima di

eliminare la chiave, è necessario decrittografare i dati o ricrittografarli con una nuova chiave KMS. Dovresti eliminare una chiave KMS solo quando hai la certezza di non doverla più utilizzare.

Ti consigliamo di configurare un CloudWatch allarme Amazon che ti avvisi se qualcuno avvia l'eliminazione di una chiave KMS. Poiché eliminare una chiave KMS è distruttivo e potenzialmente pericoloso, è AWS KMS necessario impostare un periodo di attesa e pianificare l'eliminazione in 7—30 giorni. Ciò offre l'opportunità di rivedere l'eliminazione pianificata e annullarla, se necessario.

Per maggiori informazioni, consulta le seguenti risorse:

- Pianificazione e annullamento dell'eliminazione delle chiavi nella documentazione AWS KMS
- Creazione di un allarme che rileva l'uso di una chiave KMS in attesa di eliminazione nella documentazione AWS KMS
- AWS KMS keys non deve essere eliminato involontariamente nella documentazione CSPM di Security Hub

Blocca l'accesso pubblico a AWS KMS keys

Le politiche chiave sono il modo principale per controllare l'accesso a AWS KMS keys. Ogni chiave KMS ha esattamente una policy chiave. Consentire l'accesso anonimo alle chiavi KMS può portare a una fuga di dati sensibili. Ti consigliamo di identificare tutte le chiavi KMS accessibili al pubblico e di aggiornarne le politiche di accesso per evitare richieste non firmate rivolte a queste risorse.

Per maggiori informazioni, consulta le seguenti risorse:

- Le migliori pratiche di sicurezza riportate AWS Key Management Service nella documentazione AWS KMS
- Modifica di una politica chiave nella AWS KMS documentazione
- Determinazione AWS KMS keys dell'accesso alla AWS KMS documentazione

Configura i listener di load balancer per utilizzare protocolli sicuri

Elastic Load Balancing distribuisce automaticamente il traffico delle applicazioni in entrata su più destinazioni. Puoi configurare il tuo sistema di bilanciamento del carico affinché accetti il traffico in entrata specificando uno o più listener. Un ascoltatore è un processo che controlla le richieste di connessione utilizzando il protocollo e la porta configurata. Ogni tipo di load balancer supporta protocolli e porte diversi:

- Gli Application Load Balancer prendono decisioni di routing a livello di applicazione e utilizzano i protocolli HTTP o HTTPS.
- I Network Load Balancer prendono decisioni di routing a livello di trasporto e utilizzano i protocolli TCP, TLS, UDP o TCP_UDP.
- I Classic Load Balancer prendono decisioni di routing a livello di trasporto (utilizzando i protocolli TCP o SSL) o a livello di applicazione (utilizzando i protocolli HTTP o HTTPS).

Ti consigliamo di utilizzare sempre i protocolli HTTPS o TLS. Questi protocolli assicurano che il load balancer sia responsabile della crittografia e della decrittografia del traffico tra il client e la destinazione.

Per maggiori informazioni, consulta le seguenti risorse:

- Listener per i tuoi Application Load Balancer nella documentazione di Elastic Load Balancing
- Listener per il tuo Classic Load Balancer nella documentazione di Elastic Load Balancing
- Listener per i tuoi Network Load Balancer nella documentazione di Elastic Load Balancing
- Assicurati che i AWS load balancer utilizzino protocolli di listener sicuri nella guida prescrittiva AWS
- elb-tls-https-listeners-solo nella documentazione AWS Config
- I listener Classic Load Balancer devono essere configurati con la terminazione HTTPS o TLS nella documentazione CSPM di Security Hub.
- Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS nella documentazione CSPM di Security Hub

Raccomandazioni di sicurezza per rispondere agli incidenti

Quando si verifica un evento di sicurezza nell'organizzazione, gli utenti devono essere pronti a rispondere al problema. Tutti gli utenti devono avere una conoscenza di base dei processi di risposta alla sicurezza dell'organizzazione. La pianificazione, la formazione e l'esperienza sono fondamentali per un programma di risposta agli incidenti di successo. Idealmente, preparate la vostra organizzazione prima che si verifichi un potenziale evento di sicurezza. Il AWS Well-Architected Framework identifica tre basi necessarie per un programma di risposta agli incidenti di successo nel cloud: preparazione, operazioni e attività post-incidente. Per ulteriori informazioni, vedere Aspetti della risposta agli AWS incidenti nel AWS Well-Architected Framework.

Ad eccezione dei controlli di sicurezza che notificano gli eventi o rispondono automaticamente ad essi, è possibile stabilire controlli limitati per la risposta agli incidenti. Una solida strategia di risposta agli incidenti viene stabilita principalmente attraverso i piani, i processi, i runbook, i playbook e i programmi di formazione utilizzati nell'organizzazione. È possibile utilizzare i controlli e i consigli in questa sezione per implementare le migliori pratiche per il programma di risposta agli incidenti. Per ulteriori informazioni sulle migliori pratiche per la risposta agli incidenti e le linee guida all'implementazione, vedere Incident response nel AWS Well-Architected Framework.

Consigli in questa sezione:

- Definire un piano di risposta agli incidenti
- Crea e gestisci runbook e playbook di risposta agli incidenti
- Implementa l'automazione della sicurezza basata sugli eventi
- Documenta in che modo i team operativi dovrebbero interagire con Supporto
- Configura gli avvisi per gli eventi di sicurezza

Definire un piano di risposta agli incidenti

Stabilire un piano di risposta agli incidenti (IRP) ben definito. Il piano di risposta agli incidenti è progettato per essere la base del programma di risposta agli incidenti. Questo piano deve essere personalizzato per soddisfare le esigenze di ogni organizzazione.

Per maggiori informazioni, consulta le seguenti risorse:

- Sviluppa e testa un piano di risposta agli incidenti nella AWS Security Incident Response Guide

- Sviluppa piani di gestione degli incidenti nel AWS Well-Architected Framework
- Identifica il personale chiave e le risorse esterne nel AWS Well-Architected Framework

Crea e gestisci runbook e playbook di risposta agli incidenti

Una parte fondamentale della preparazione ai processi di risposta agli incidenti è lo sviluppo di playbook. I playbook di risposta agli incidenti forniscono una serie di passaggi consigliati che gli utenti devono seguire quando si verifica un evento di sicurezza. Avere una struttura e dei passaggi chiari semplifica la risposta e riduce la probabilità di errore umano.

Per maggiori informazioni, consulta le seguenti risorse:

- Per cosa creare dei playbook nella AWS Security Incident Response Guide
- AWS esempi di playbook sulla risposta agli incidenti su GitHub
- Sviluppa e testa i playbook di risposta agli incidenti di sicurezza nel AWS Well-Architected Framework

Implementa l'automazione della sicurezza basata sugli eventi

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

Molti supportano le risposte automatiche. Servizi AWS Ad esempio, puoi configurare un CloudWatch allarme Amazon per parametri specifici e l'allarme può avviare un'azione quando l'allarme cambia stato. Tramite Amazon EventBridge, puoi anche configurare la risposta e la correzione automatiche per i risultati in Amazon AWS Security Hub CSPM Inspector.

Per ulteriori informazioni, consulta le seguenti risorse:

- Correggi automaticamente i risultati di sicurezza di Amazon Inspector nel AWS blog sulla sicurezza
- Inizia a utilizzare l'automazione della risposta alla sicurezza AWS nel Security Blog AWS
- Risposta di sicurezza automatizzata attiva AWS nella AWS Solutions Library
- Utilizzo degli CloudWatch allarmi Amazon nella documentazione CloudWatch

- Risposta e correzione automatizzate nella documentazione CSPM di Security Hub
- Creazione di risposte personalizzate ai risultati di Amazon Inspector con Amazon EventBridge nella documentazione di Amazon Inspector

Documenta in che modo i team operativi dovrebbero interagire con Supporto

Per voi Account AWS, potete definire un contatto principale e tre contatti alternativi. Ti consigliamo di fornire un contatto di sicurezza per ciascuna Account AWS o per la tua organizzazione.

Supporto AWS offre una gamma di piani che forniscono l'accesso a strumenti e competenze in grado di supportare il successo e lo stato operativo delle AWS soluzioni. Inoltre, valuta se la tua organizzazione trarrebbe vantaggio dall'utilizzo di un piano AWS Managed Services anziché di un Supporto piano. AWS Managed Services (AMS) ti aiuta a operare in modo più efficiente e sicuro fornendo una gestione continua dell' AWS infrastruttura, tra cui monitoraggio, gestione degli incidenti, indicazioni sulla sicurezza, supporto patch e backup per i carichi di AWS lavoro. Il modello di supporto AMS può essere più adatto per le organizzazioni che dispongono di risorse limitate nei propri team operativi sul cloud. Ti consigliamo di confrontare questi modelli e piani per scegliere quello più adatto al caso d'uso della tua organizzazione e al livello di maturità del cloud.

Per maggiori informazioni, consulta le seguenti risorse:

- Scopri i team di AWS risposta e il supporto nella AWS Security Incident Response Guide
- Aggiorna i tuoi contatti alternativi Account AWS nella Guida alla gestione AWS dell'account
- Confronta Supporto i piani sul sito web AWS
- Strategia AWS Managed Services da utilizzare per raggiungere i risultati aziendali prefissati in AWS Prescriptive Guidance

Configura gli avvisi per gli eventi di sicurezza

Il rilevamento di un'anomalia è importante quanto le misure implementate per controllarla. L'avviso è il componente principale della fase di rilevamento. Genera una notifica per avviare il processo di risposta all'incidente in base Account AWS all'attività di interesse. Assicurati che gli avvisi includano informazioni pertinenti per consentire al team di intervenire.

Per maggiori informazioni, consulta le seguenti risorse:

- Rilevamento nella AWS Security Incident Response Guide
- Prepara le funzionalità forensi nel Well-Architected AWS Framework
- Implementa eventi di sicurezza utilizzabili nel Well-Architected AWS Framework

Fasi successive

Mentre prosegui nel tuo percorso verso il cloud, è importante applicare questi controlli documentati, linee guida e opzioni di correzione. Questi consigli aiutano a migliorare la vostra posizione di sicurezza nel cloud e ad adempiere alle vostre responsabilità in materia di sicurezza nell'ambito del modello di responsabilità condivisa Cloud AWS, come definito nel modello di responsabilità AWS condivisa.

Per i passaggi successivi, consigliamo quanto segue:

- Per ulteriori informazioni sulle best practice e sulle linee guida all'implementazione, consulta i sei pilastri del AWS Well-Architected Framework.
- Per quanto riguarda Servizi AWS i controlli utilizzati dalla tua organizzazione, esamina l'elenco dei AWS Security Hub CSPM controlli disponibili e valuta se è necessario abilitare qualcuno di questi controlli nel tuo ambiente.
- Per quanto riguarda Servizi AWS le regole utilizzate dall'organizzazione, esaminate l'elenco delle regole AWS Config gestite disponibili e valutate se è necessario abilitare qualcuna di queste regole nel vostro ambiente.

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
MFA per utente root	Abbiamo aggiornato i consigli e fornito ulteriori informazioni nella sezione MFA per l'utente root.	9 novembre 2023
Pubblicazione iniziale	—	27 ottobre 2023

AWS Glossario delle linee guida prescrittive

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

Numeri

7 R

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

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

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

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

migrazione attiva-passiva

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

funzione di aggregazione

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

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

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

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

AWS Workload Qualification Framework (WQF)AWS

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

B

bot difettoso

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

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

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

Classificazione binaria

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

filtro Bloom

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

implementazione blu/verde

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

bot

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

botnet

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

ramo

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

accesso break-glass

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

strategia brownfield

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

cache del buffer

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

capacità di business

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

pianificazione della continuità operativa (BCP)

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

C

CAF

Vedi Cloud Adoption AWS Framework.

implementazione canaria

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

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

Centro di eccellenza cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

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

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

CMDB

Vedi database di gestione della configurazione.

repository di codice

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

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

cache fredda

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

dati freddi

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

visione artificiale (CV)

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

deriva della configurazione

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

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

Il processo di automazione delle fasi di origine, compilazione, test, gestione temporanea e produzione del processo di rilascio del software. CI/CD viene comunemente descritto come una pipeline. CI/CD può aiutarvi ad automatizzare i processi, migliorare la produttività, migliorare

la qualità del codice e velocizzare le consegne. Per ulteriori informazioni, consulta Vantaggi della distribuzione continua. CD può anche significare continuous deployment (implementazione continua). Per ulteriori informazioni, consulta Distribuzione continua e implementazione continua a confronto.

CV

Vedi visione artificiale.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

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

deriva dei dati

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

dati in transito

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

rete di dati

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di definizione del database.

deep ensemble

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

deep learning

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

defense-in-depth

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

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

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

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

gemello digitale

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

tabella delle dimensioni

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

disastro

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

disaster recovery (DR)

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

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

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

DOTT.

Vedi disaster recovery.

rilevamento della deriva

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

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

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

scambio elettronico di dati (EDI)

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

crittografia

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

chiave crittografica

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

endianità

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

endpoint

Vedi service endpoint.

servizio endpoint

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

pianificazione delle risorse aziendali (ERP)

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

crittografia envelope

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

ambiente

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

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

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

epica

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

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

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

F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

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

prompt con pochi scatti

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

Vedi modello di base.

modello di fondazione (FM)

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

G

IA generativa

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

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

immagine dorata

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

strategia greenfield

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

guardrail

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

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

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

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

alta disponibilità (HA)

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

modernizzazione storica

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

dati di blocco

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

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

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

I

IaC

Vedi l'infrastruttura come codice.

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

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

VPC in ingresso (ingress)

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

migrazione incrementale

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

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

IIoInternet delle cose industriale (T)

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

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

modello linguistico di grandi dimensioni (LLM)

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

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

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

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

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

ramo principale

Vedi filiale.

malware

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

servizi gestiti

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

sistema di esecuzione della produzione (MES)

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

MAP

Vedi Migration Acceleration Program.

meccanismo

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

account membro

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

MEH

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

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

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

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

migrazione su larga scala

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

fabbrica di migrazione

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

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

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

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

Vedi machine learning.

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

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

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

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

infrastruttura mutabile

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

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

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

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

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

OPC-UA

Vedi Open Process Communications - Unified Architecture.

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

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

tecnologia operativa (OT)

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

integrazione delle operazioni (OI)

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

trail organizzativo

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

gestione del cambiamento organizzativo (OCM)

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

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

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

ORR

Vedi la revisione della prontezza operativa.

NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

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

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

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

persistenza poliglotta

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

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

concatenamento rapido

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

pseudonimizzazione

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

publish/subscribe (pub/sub)

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

Q

Piano di query

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

regressione del piano di query

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

R

Matrice RACI

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

RAG

Vedi Retrieval Augmented Generation.

ransomware

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

Matrice RASCI

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

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

Region

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

regressione

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

riospitare

Vedi 7 R.

rilascio

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

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

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

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi obiettivo del punto di ripristino.

VERSO

Vedi obiettivo del tempo di ripristino.

runbook

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

S

SAML 2.0

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

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

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

sicurezza fin dalla progettazione

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

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

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

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

Modello di responsabilità condivisa

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

SIEM

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

punto di errore singolo (SPOF)

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

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

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

SPOF

Vedi punto di errore singolo.

schema a stella

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

modello del fico strangolatore

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

sottorete

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

controllo di supervisione e acquisizione dati (SCADA)

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

crittografia simmetrica

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

test sintetici

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

prompt di sistema

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

T

tag

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

variabile di destinazione

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

elenco di attività

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

ambiente di test

Vedi ambiente.

training

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

Transit Gateway

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

flusso di lavoro basato su trunk

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

Accesso attendibile

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

regolazione

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

team da due pizze

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

U

incertezza

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

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.