Passaggio al multiplo Account AWS

AWS Guida prescrittiva

AWS Guida prescrittiva: Passaggio al multiplo Account AWS

Table of Contents

Passaggio al multiplo Account AWS

Amazon Web Services (collaboratori)

Novembre 2024 (cronologia dei documenti)

Molte aziende iniziano il loro percorso utilizzando un unico account Amazon Web Services (AWS). Più ruoli all'interno di un'azienda utilizzano questo account per gestire l'attività. Gli ingegneri sviluppano il codice, lo implementano in ambienti di sviluppo e test e promuovono modifiche alla produzione. I product manager interrogano le origini dati per raccogliere informazioni sulle prestazioni aziendali. Il team di vendita sta effettuando dimostrazioni dall'ambiente di produzione per attirare nuovi clienti. Il team finanziario sta monitorando la spesa per il cloud dalla AWS Billing console.

Quando tutti questi ruoli separati ne utilizzano uno solo Account AWS, può diventare difficile applicare la best practice di sicurezza basata sull'applicazione delle autorizzazioni con privilegi minimi, il che significa che si concedono solo le autorizzazioni minime necessarie per svolgere il lavoro. A un certo punto dello sviluppo di una startup, qualcuno farà la domanda Tutti i nostri ingegneri hanno bisogno di accedere alla produzione? La risposta è quasi sempre no, ma molte aziende hanno difficoltà a trasformare l'ambiente esistente con un unico account in un ambiente multi-account senza rallentare l'attività.

Questa guida illustra le best practice per aiutarti a passare da un ambiente con account singolo a un ambiente multi-account. Descrive le decisioni da prendere in merito alla migrazione degli account, alla gestione degli utenti, al networking, alla sicurezza e all'architettura. È progettato per aiutarti ad avere successo con tempi di inattività minimi o nulli per l'azienda e le operazioni quotidiane. Questa guida si concentra sulle seguenti funzionalità durante la transizione da un ambiente con account singolo a uno con più account: Account AWS

- Gestione delle identità e controllo degli accessi
- Gestione delle autorizzazioni e dell'accesso
- Connettività di rete
- Risposta agli incidenti di sicurezza
- Backup
- Migrazione nell'account
- Migrazione delle risorse
- Considerazioni sulla fatturazione

Per ulteriori informazioni sulle funzionalità, consulta Cloud Foundation su AWS.

Questa guida è allineata alle risorse esistenti relative a questo argomento, tra cui lo AWS Startup Security Baseline (AWS SSB), il white paper Organizing Your AWS Environment Using Multiple Accounts, il AWS Security Reference Architecture (AWS SRA) e il white paper Establishing Your Cloud Foundation on. AWS È necessario continuare a utilizzare tali risorse per indicazioni più specifiche non trattate in questa guida.

Destinatari principali

Questa guida è la soluzione ideale per le aziende che desiderano o devono passare a più Account AWS. Per le startup, questa esigenza si presenta in genere quando si è trovata la soluzione più adatta al mercato del prodotto, raccolto un round di finanziamenti e si inizia ad assumere discipline ingegneristiche distinte, come l'infrastruttura, le operazioni di sviluppo (DevOps) o la sicurezza.

Anche se la tua azienda non è pronta per questa transizione, puoi comunque utilizzare questa guida per comprendere le decisioni da prendere durante la transizione e iniziare a prepararti.

Obiettivi per la transizione verso un'architettura multi-account

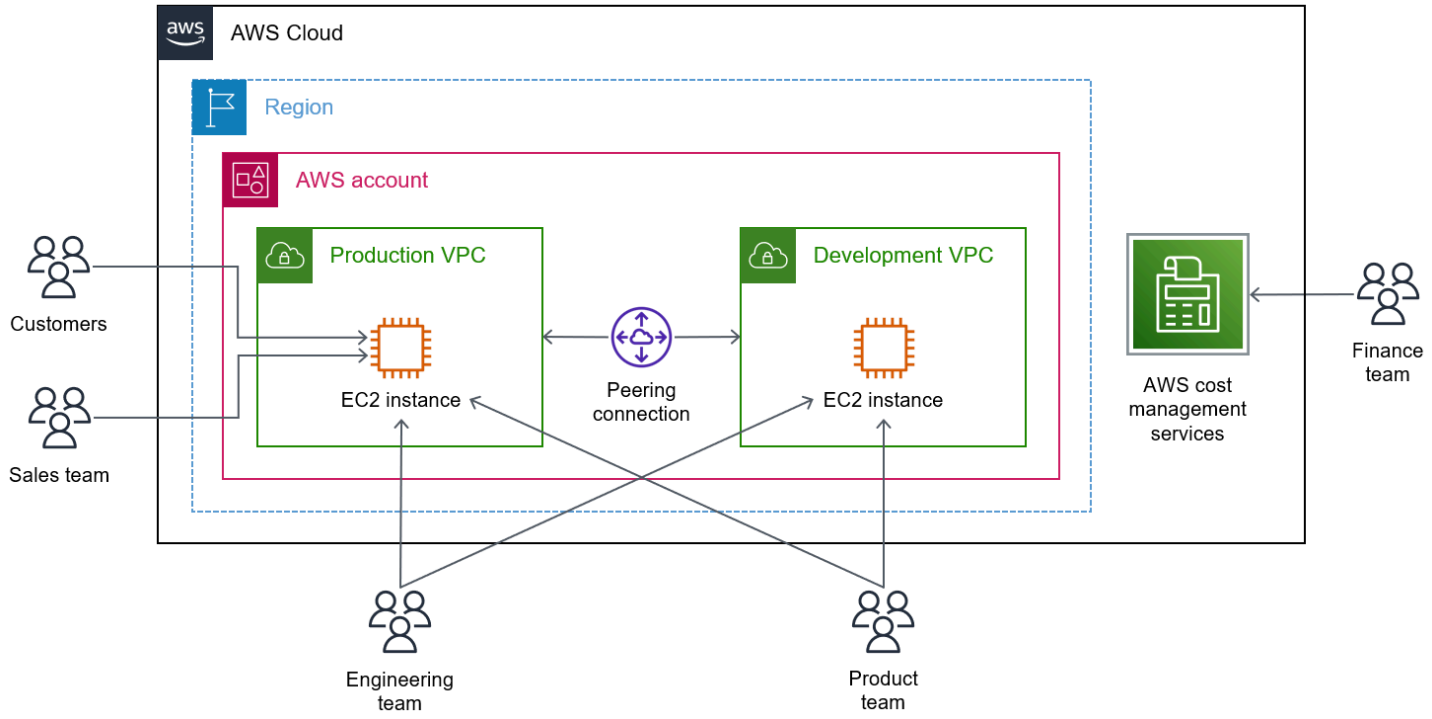
La transizione verso un'architettura multi-account è in genere determinata dall'esigenza aziendale di ottenere uno o più dei seguenti vantaggi:

- Raggruppamento dei carichi di lavoro in base allo scopo o alla proprietà dell'azienda
- Applicazione di controlli di sicurezza distinti per ambiente
- Limitazione dell'accesso ai dati sensibili
- Promozione dell'innovazione e dell'agilità
- Limitazione dell'ambito di impatto degli eventi avversi
- Supporto di più modelli operativi IT
- Gestione dei costi
- Distribuzione delle Servizio AWS quote e dei limiti di frequenza delle richieste API

Per ulteriori informazioni sui numerosi vantaggi dell'utilizzo di un'architettura multi-account, consulta Organizzare AWS l'ambiente utilizzando più account (AWS white paper) e Linee guida per configurare un ambiente ben progettato (documentazione).AWS Control Tower

Esempio di architettura con account singolo

Come punto di partenza, è normale che le startup o le piccole aziende utilizzino un singolo cloud privato virtuale (VPCs) Regione AWS e dispongano di due cloud privati virtuali collegati tramite peering VPC. Ogni VPC contiene risorse di elaborazione, come istanze Amazon Elastic Compute Cloud (Amazon). EC2 Il team di progettazione sviluppa il codice direttamente nel VPC di sviluppo. Il team di prodotto esamina le modifiche, quindi il team di progettazione promuove manualmente le modifiche al VPC di produzione. Il team finanziario ha accesso al file in modo da Account AWS poter rivedere la console. Gestione dei costi e fatturazione AWS



Di seguito sono riportati alcuni esempi di sfide che un'azienda potrebbe incontrare in questo ambiente:

- Un ingegnere ha erroneamente eliminato i dati di produzione pensando di accedere a un database di sviluppo.
- Una dimostrazione di vendita ne ha risentito quando un'implementazione in produzione ha richiesto più tempo del previsto.
- Durante il test di caricamento del codice di sviluppo, il VPC di produzione è diventato lento e ha generato messaggi di errore relativi alla limitazione.
- Il team finanziario non è in grado di differenziare i costi per gli ambienti di produzione e di sviluppo.
- Il CEO teme che alcuni appaltatori esteri appena assunti abbiano accesso ai dati dei clienti tramite il VPC di produzione.
- Il team finanziario non può impedire l'accesso a informazioni specifiche Servizi AWS che potrebbero comportare costi elevati.

L'adozione di una strategia multi-account risolve tutte queste sfide utilizzando sistemi Account AWS compartimentati per separare carichi di lavoro e accessi.

Framework di base e responsabilità di sicurezza per la transizione a un'architettura multi-account

Le informazioni e le best practice contenute in questa guida sono concepite per integrare i consigli AWS esistenti per l'infrastruttura e la sicurezza. Durante la transizione da uno Account AWS a uno multiplo Account AWS, è importante assicurarsi che la nuova architettura multi-account sia coerente con i principi AWS Well-Architected Framework e Cloud Foundation. Questo ti aiuta a creare e gestire un ambiente progettato per la sicurezza, le prestazioni e la resilienza, rispettando al contempo i requisiti di governance e le migliori pratiche. AWS

AWS Well-Architected Framework

AWS Well-Architected Framework ti aiuta a creare un'infrastruttura sicura, ad alte prestazioni, resiliente ed efficiente per applicazioni e carichi di lavoro. Questa guida si allinea ai pilastri di eccellenza operativa, sicurezza e affidabilità di questo framework. Questo ti aiuta a soddisfare i requisiti aziendali e normativi seguendo le raccomandazioni attuali. AWS

Puoi valutare la tua aderenza alle best practice di Well-Architected utilizzando AWS Well-Architected Tool nel tuo Account AWS.

Cloud Foundation su AWS

Stabilire Your Cloud Foundation su AWS (AWS Whitepaper) fornisce indicazioni che consentono di personalizzare AWS l'ambiente per soddisfare le esigenze della propria azienda. Utilizzando un approccio basato sulle funzionalità, puoi creare un ambiente per l'implementazione, il funzionamento e la gestione dei carichi di lavoro. Puoi anche migliorare le capacità di estendere il tuo ambiente man mano che i requisiti evolvono e distribuire carichi di lavoro aggiuntivi nel cloud. Per ulteriori informazioni sulle 30 funzionalità definite da AWS, consulta Capabilities. Questa guida include le best practice per implementare le funzionalità iniziali nell'ordine previsto.

Puoi adottare e implementare funzionalità in base alle tue esigenze operative e di governance. Man mano che i requisiti aziendali maturano, l'approccio basato sulle funzionalità può essere utilizzato come meccanismo per verificare che l'ambiente cloud sia pronto a supportare i carichi di lavoro e a scalare in base alle esigenze. Questo approccio ti consente di creare con sicurezza il tuo ambiente cloud per i tuoi sviluppatori e la tua azienda.

Gestione delle identità e controllo degli accessi per la transizione a un'architettura multi-account

La prima fase della transizione a un'architettura multi-account consiste nel configurare la nuova struttura degli account all'interno di un'organizzazione. Quindi puoi aggiungere utenti e configurare il loro accesso agli account. Questa sezione descrive gli approcci per la gestione dell'accesso umano in più Account AWS.

Questa sezione contiene le attività seguenti:

- Configurazione di un'organizzazione
- Creazione di una zona di destinazione
- Aggiunta di unità organizzative
- Aggiunta di utenti iniziali
- Gestisci gli account membri

Configurazione di un'organizzazione

Se ne hai più Account AWS, puoi gestire logicamente tali account tramite un'organizzazione in AWS Organizations. Un account in AWS Organizations è uno standard Account AWS che contiene AWS le tue risorse e le identità che possono accedere a tali risorse. Un'organizzazione è un'entità che consolida le tue informazioni Account AWS in modo da poterle amministrare come un'unica unità.

Quando utilizzi un account per creare un'organizzazione, tale account diventa l'account di gestione (noto anche come account di pagamento o account root) per l'organizzazione. Un'organizzazione può avere un solo account di gestione. Quando ne aggiungi altri Account AWS all'organizzazione, questi diventano account membro.

> **Note**
>
> Ciascuno ha Account AWS anche un'unica identità chiamata utente root. Puoi accedere come utente root utilizzando l'indirizzo e-mail e la password usati per creare l'account. Ti consigliamo tuttavia di non utilizzare l'utente root per le attività quotidiane, anche quelle amministrative. Per ulteriori informazioni, consulta la sezione Utente root Account AWS.

Consigliamo inoltre di centralizzare l'accesso root per gli account dei membri e di rimuovere le credenziali dell'utente root dagli account dei membri dell'organizzazione.

Gli account vengono organizzati in una struttura gerarchica ad albero composta dall'area principale dell'organizzazione, dalle unità organizzative () e dagli account dei membri. OUs Il root è il container genitore per tutti gli account dell'organizzazione. Un'unità organizzativa (UO) è un container per account all'interno della root. Un'unità organizzativa può contenere account di altri membri o di altri membri OUs . Una UO può avere esclusivamente un genitore e attualmente ogni account può essere membro di una sola UO. Per ulteriori informazioni, vedere Terminologia e concetti (AWS Organizations documentazione).

Una policy di controllo dei servizi (SCP) specifica i servizi e le azioni che gli utenti e i ruoli possono utilizzare. SCPs sono simili alle politiche di autorizzazione AWS Identity and Access Management (IAM) tranne per il fatto che non concedono autorizzazioni. SCPs Definisci invece le autorizzazioni massime. Quando alleghi una policy a uno dei nodi della gerarchia, questa si applica a tutti gli account OUs e agli account all'interno di quel nodo. Ad esempio, se si applica una politica alla radice, questa si applica a tutti gli OUsaccount dell'organizzazione e se si applica una politica a un'unità organizzativa, si applica solo agli account OUs e nell'unità organizzativa di destinazione.

Una politica di controllo delle risorse (RCP) offre il controllo centralizzato sulle autorizzazioni massime disponibili per le risorse dell'organizzazione. RCPs ti aiuta a garantire che le risorse del tuo account rispettino le linee guida per il controllo degli accessi dell'organizzazione.

Puoi utilizzare la AWS Organizations console per visualizzare e gestire centralmente tutti i tuoi account all'interno di un'organizzazione. Uno dei vantaggi dell'utilizzo di un'organizzazione è la possibilità di ricevere una fattura consolidata che riporta tutti i costi associati agli account di gestione e dei membri. Per ulteriori informazioni, consulta Fatturazione consolidata (AWS Organizations documentazione).

Best practice

- Non utilizzarne uno esistente Account AWS per creare un'organizzazione. Inizia con un nuovo account, che diventerà il tuo account di gestione dell'organizzazione. Le operazioni privilegiate possono essere eseguite all'interno dell'account di gestione di un'organizzazione SCPs e RCPs non si applicano all'account di gestione. Ecco perché dovresti limitare le risorse e i dati cloud contenuti nell'account di gestione solo a quelli che devono essere gestiti in tale account.

- Limita l'accesso all'account di gestione solo alle persone che devono fornire nuovi account Account AWS e amministrare l'organizzazione.
- Viene utilizzato SCPs per definire le autorizzazioni massime per gli account root, le unità organizzative e gli account dei membri. SCPs non può essere applicato direttamente all'account di gestione.
- Utilizzato RCPs per definire le autorizzazioni massime per le risorse negli account dei membri. RCPsnon può essere applicato direttamente all'account di gestione.
- Rispetta le migliori pratiche per AWS Organizations (AWS Organizations documentazione).

Creazione di una zona di destinazione

Una landing zone è un AWS ambiente multi-account ben progettato che rappresenta un punto di partenza dal quale è possibile distribuire carichi di lavoro e applicazioni. Fornisce un punto di riferimento per iniziare a utilizzare l'architettura multi-account, la gestione delle identità e degli accessi, la governance, la sicurezza dei dati, la progettazione della rete e la registrazione. AWS Control Tower è un servizio che semplifica la manutenzione e la governance di un ambiente multi-account fornendo guardrail automatizzati. In genere, si effettua il provisioning di un'unica AWS Control Tower landing zone che gestisce l'ambiente in tutti gli ambienti Regioni AWS. AWS Control Tower funziona orchestrando altri elementi Servizi AWS all'interno del tuo account. Per ulteriori informazioni, consulta Cosa succede quando si imposta una landing zone (AWS Control Tower documentazione).

Quando configuri una landing zone con AWS Control Tower, identifichi tre account condivisi: l'account di gestione, l'account di archiviazione dei log e l'account di controllo. Per ulteriori informazioni, consulta Cosa sono gli account condivisi (AWS Control Tower documentazione). Per l'account di gestione, devi utilizzare un account esistente che non ospita carichi di lavoro per configurare la zona di destinazione. Per l'archivio dei log e gli account di controllo, puoi scegliere di riutilizzare gli account esistenti Account AWS o AWS Control Tower crearli automaticamente.

Per istruzioni su come configurare la AWS Control Tower landing zone, consulta Guida introduttiva (AWS Control Tower documentazione).

Best practice

- Attieniti alle migliori pratiche contenute nei principi di progettazione per la tua strategia multi-account (AWS Whitepaper).

- Rispetta le migliori pratiche per gli amministratori (documentazione). AWS Control Tower AWS Control Tower
- Crea la tua landing zone nell'area Regione AWS che ospita la maggior parte dei tuoi carichi di lavoro.

> **Important**
>
> Se decidi di cambiare questa regione dopo aver dispiegato la tua landing zone, hai bisogno dell' Supporto AWS assistenza e devi disattivare la zona di atterraggio. Questa pratica non è consigliata.

- Per determinare quali regioni AWS Control Tower governeranno, seleziona solo le regioni in cui prevedi di distribuire immediatamente i carichi di lavoro. Puoi modificare queste regioni o aggiungerne altre in un secondo momento. Se AWS Control Tower governa una Regione, schiererà i suoi guardrail investigativi in quella Regione come. Regole di AWS Config
- Dopo aver determinato quali Regioni AWS Control Tower governeranno, nega l'accesso a tutte le Regioni non governate. In questo modo, puoi garantire che i carichi di lavoro e gli sviluppatori possano utilizzare solo le Regioni AWS approvate. Questa pratica è implementata come una policy di controllo dei servizi (SCP) nell'organizzazione. Per ulteriori informazioni, consulta Configurare il controllo di Regione AWS rifiuto (documentazione).AWS Control Tower
- Quando configuri la landing zone in AWS Control Tower, ti consigliamo di rinominare quanto segue OUs e gli account:
  - Ti consigliamo di rinominare l'UO Security in Security_Prod per indicare che questa UO verrà utilizzata per Account AWS legati alla sicurezza della produzione.
  - Ti consigliamo di consentire la creazione AWS Control Tower di un'unità organizzativa aggiuntiva e quindi di rinominarla da Sandbox a Workloads. Nella sezione successiva, ne creerai altre OUs all'interno dell'unità organizzativa Workloads, che utilizzerai per organizzare le tue. Account AWS
  - Si consiglia di rinominare la registrazione centralizzata Account AWS da Log Archive a. log-archive-prod
  - Si consiglia di rinominare l'account di controllo da Audit a. security-tooling-prod
- Per prevenire le frodi, è AWS necessario Account AWS disporre di una cronologia di utilizzo prima di poter essere aggiunti a una AWS Control Tower landing zone. Se ne utilizzi una nuova Account AWS senza alcuna cronologia di utilizzo, nel nuovo account puoi avviare un'istanza Amazon Elastic Compute Cloud (Amazon EC2) che non è nel piano AWS gratuito. Lascia che l'istanza venga eseguita per qualche minuto, quindi terminala.

Aggiunta di unità organizzative

Stabilire la struttura organizzativa adeguata è fondamentale per la creazione di un ambiente multi-account. Poiché utilizzi le policy di controllo del servizio (SCPs) per definire le autorizzazioni massime per un'unità organizzativa e gli account al suo interno, la struttura organizzativa deve essere logica dal punto di vista della gestione, delle autorizzazioni e dei report finanziari. Per ulteriori informazioni sulla struttura di un'organizzazione, incluse le unità organizzative (OUs), vedere Terminologia e concetti (AWS Organizations documentazione).

In questa sezione, personalizzi la landing zone creando nidi OUs che ti aiutano a segmentare e strutturare i tuoi ambienti, come quelli di produzione e non produzione. Queste best practice consigliate sono progettate per segmentare la zona di destinazione in modo da separare le risorse di produzione da quelle non di produzione e separare l'infrastruttura dai carichi di lavoro.

Per ulteriori informazioni su come creare OUs, consulta Gestione delle unità organizzative (AWS Organizations documentazione).

Best practice

- All'interno dell'unità organizzativa Workloads in cui hai creatoCreazione di una zona di destinazione, crea quanto segue annidato OUs:
  - Prod: utilizza questa UO per gli Account AWS che archiviano e accedono ai dati di produzione, inclusi i dati dei clienti.
  - NonProd— Utilizzate questa unità organizzativa per Account AWS archiviare dati non di produzione, come ambienti di sviluppo, gestione temporanea o test

Nella root dell'organizzazione, crea una UO Infrastructure_Prod. Utilizza questa UO per ospitare un account di rete centralizzato.

Aggiunta di utenti iniziali

Esistono due modi per concedere alle persone l'accesso agli Account AWS:

- Identità IAM, come utenti, gruppi e ruoli
- Federazione delle identità, ad esempio utilizzando AWS IAM Identity Center

Nelle aziende più piccole e negli ambienti con account singolo, è normale che gli amministratori creino un utente IAM quando una nuova persona entra a far parte dell'azienda. La chiave di accesso e le credenziali della chiave segreta associate a un utente IAM sono note come credenziali a lungo termine perché non scadono. Tuttavia, questa non è una best practice di sicurezza consigliata perché se un utente malintenzionato compromettesse tali credenziali, dovresti generare un nuovo set di credenziali per l'utente. Un altro approccio per l'accesso Account AWS è tramite i ruoli IAM. Puoi anche utilizzare AWS Security Token Service (AWS STS) per richiedere temporaneamente credenziali a breve termine che scadono dopo un periodo di tempo configurabile.

Puoi gestire l'accesso delle persone al tuo Account AWS tramite IAM Identity Center. Puoi creare account utente individuali per ciascuno dei tuoi dipendenti o collaboratori, che possono gestire le proprie password e soluzioni di autenticazione a più fattori (MFA) e tu puoi raggrupparli per gestire l'accesso. Quando si configura l'MFA, è possibile utilizzare token software, ad esempio applicazioni di autenticazione, oppure è possibile utilizzare token hardware, come i dispositivi. YubiKey

IAM Identity Center supporta anche la federazione da provider di identità esterni (IdPs) come Okta e Ping Identity. JumpCloud Per ulteriori informazioni, consulta la sezione Gestori delle identità supportati (documentazione di Centro identità IAM). Effettuando la federazione con un IdP esterno, puoi gestire l'autenticazione degli utenti tra le applicazioni e quindi utilizzare IAM Identity Center per autorizzare l'accesso a specifiche applicazioni. Account AWS

Best practice

- Aderisci alle Best practice relative alla sicurezza (documentazione IAM) per configurare l'accesso degli utenti.
- Gestisci l'accesso all'account per gruppi anziché per singoli utenti. In Centro identità IAM, crea nuovi gruppi che rappresentino ciascuna delle tue funzioni aziendali. Ad esempio, potresti creare gruppi per l'ingegneria, la finanza, le vendite e la gestione dei prodotti.
- Spesso, i gruppi vengono definiti separando coloro che hanno bisogno di accedere a tutti gli Account AWS (spesso accesso in sola lettura) e coloro che necessitano dell'accesso a un unico Account AWS. Ti consigliamo di utilizzare la seguente convenzione di denominazione per i gruppi in modo che sia facile identificare le autorizzazioni Account AWS e le autorizzazioni associate al gruppo.

  `<prefix>-<account name>-<permission set>`
- Ad esempio, per il gruppo `AWS-A-dev-nonprod-DeveloperAccess`, `AWS-A` è un prefisso che indica l'accesso a un singolo account, `dev-nonprod` è il nome dell'account e `DeveloperAccess` è il set di autorizzazioni assegnato al gruppo. Per il gruppo `AWS-O-BillingAccess`, il prefisso

`AWS-0` indica l'accesso all'intera organizzazione e `BillingAccess` indica il set di autorizzazioni per il gruppo. In questo esempio, poiché il gruppo ha accesso all'intera organizzazione, il nome dell'account non è rappresentato nel nome del gruppo.

- Se utilizzi Centro identità IAM con un IdP esterno basato su SAML e desideri richiedere l'MFA, puoi utilizzare il controllo degli accessi basato su attributi (ABAC) per passare il metodo di autenticazione dall'IdP a Centro identità IAM. Gli attributi vengono inviati tramite le asserzioni SAML. Per ulteriori informazioni, consulta la sezione Abilitazione e configurazione degli attributi per il controllo degli accessi (documentazione di Centro identità IAM).

  Molti IdPs, come Microsoft Azure Active Directory e Okta, possono utilizzare l'attestazione Authentication Method Reference (`amr`) all'interno di un'asserzione SAML per passare lo stato MFA dell'utente a IAM Identity Center. L'attestazione utilizzata per affermare lo stato di MFA e il relativo formato variano in base all'IdP. Per ulteriori informazioni, consulta la documentazione relativa al tuo IdP.

  In IAM Identity Center, puoi quindi creare policy di set di autorizzazioni che determinano chi può accedere alle tue risorse. AWS Quando abiliti l'ABAC e specifichi gli attributi, Centro identità IAM trasmette il valore degli attributi dell'utente autenticato a IAM per l'utilizzo nella valutazione delle policy. Per ulteriori informazioni, consulta la sezione Creazione di policy di autorizzazione per ABAC (documentazione di Centro identità IAM). Come illustrato nel seguente esempio, utilizzi la chiave di condizione `aws:PrincipalTag` per creare una regola di controllo di accesso per l'MFA.

```
"Condition": {
  "StringLike": { "aws:PrincipalTag/amr": "mfa" }
}
```

Gestisci gli account membri

In questa sezione inviti i tuoi account preesistenti nell'organizzazione e inizi a creare nuovi account all'interno della tua organizzazione. Una parte importante di questo processo è la definizione dei criteri da utilizzare per determinare se è necessario fornire un nuovo account.

Questa sezione contiene le attività seguenti:

- Invita il tuo account preesistente
- Personalizza le impostazioni del VPC in AWS Control Tower
- Definizione dei criteri di determinazione dell'ambito

Invita il tuo account preesistente

All'interno AWS Organizations, puoi invitare l'account preesistente della tua azienda nella tua nuova organizzazione. Solo l'account di gestione dell'organizzazione può invitare altri account a iscriversi. Nel momento in cui l'amministratore di un account invitato accetta, l'account di gestione di tale organizzazione diventa responsabile per tutte le spese maturate dal nuovo account membro. Per ulteriori informazioni, consulta la sezione Invito a un Account AWS per entrare a far parte dell'organizzazione e Accettazione o rifiuto di un invito da un'organizzazione (documentazione AWS Organizations).

> **Note**
>
> Puoi invitare un account a entrare a far parte di un'organizzazione solo se tale account non appartiene attualmente a un'altra organizzazione. Se l'account è membro di un'organizzazione esistente, devi rimuoverlo dall'organizzazione. Se l'account è l'account di gestione di un'altra organizzazione creata per errore, è necessario eliminare l'organizzazione.

> **Important**
>
> Se hai bisogno di accedere a informazioni storiche sui costi o sull'utilizzo dal tuo account preesistente, puoi usarle AWS Cost and Usage Report per esportare tali informazioni in un bucket Amazon Simple Storage Service (Amazon S3). Fallo prima di accettare l'invito a unirti a un'organizzazione. Quando un account entra a far parte di un'organizzazione, perdi l'accesso a questi dati storici relativi all'account. Per ulteriori informazioni, consulta la sezione Configurazione di un bucket Amazon S3 per i report di costi e utilizzo (documentazione AWS Cost and Usage Report).

Best practice

- Ti consigliamo di aggiungere il tuo account preesistente, che probabilmente contiene carichi di lavoro di produzione, all'unità organizzativa Workloads>Prod che hai creato inAggiunta di unità organizzative .
- Per impostazione predefinita, l'account di gestione dell'organizzazione non dispone dell'accesso amministrativo agli account membri invitati all'organizzazione. Se desideri che l'account di gestione abbia il controllo amministrativo, devi creare il ruolo OrganizationAccountAccessRoleIAM

nell'account membro e concedere l'autorizzazione all'account di gestione per assumere il ruolo. Per ulteriori informazioni, consulta Creazione OrganizationAccountAccessRole di un account membro invitato (AWS Organizations documentazione).

- Per l'account preesistente che hai invitato a far parte dell'organizzazione, consulta le migliori pratiche per gli account dei membri (AWS Organizations documentazione) e conferma che l'account rispetti questi consigli.

Personalizza le impostazioni del VPC in AWS Control Tower

Ti consigliamo di effettuare il provisioning di nuovi Account AWS prodotti tramite Account Factory in AWS Control Tower. Utilizzando Account Factory, puoi utilizzare l' AWS Control Tower integrazione con Amazon EventBridge per fornire nuove risorse non Account AWS appena l'account viene creato.

Quando si configura un nuovo Account AWScloud privato virtuale (VPC) predefinito viene fornito automaticamente. Tuttavia, quando crei un nuovo account tramite Account Factory, AWS Control Tower effettua automaticamente il provisioning di un VPC aggiuntivo. Per ulteriori informazioni, vedere Panoramica AWS Control Tower e VPCs (AWS Control Tower documentazione). Ciò significa che, per impostazione predefinita, due AWS Control Tower disposizioni predefinite VPCs in ogni nuovo account.

È normale che le aziende desiderino un maggiore controllo all' VPCs interno dei propri conti. Molti preferiscono utilizzare altri servizi AWS CloudFormation, come Hashicorp Terraform o Pulumi, per configurare e gestire i propri. VPCs È necessario personalizzare le impostazioni di Account Factory per impedire la creazione del VPC aggiuntivo fornito da AWS Control Tower. Per istruzioni, consulta Configurare le impostazioni di Amazon VPC (AWS Control Tower documentazione) e applicare le seguenti impostazioni:

1. Disabilita l'opzione Sottorete accessibile da Internet.
2. In Numero massimo di sottoreti private, scegli 0.
3. In Regioni per la creazione di VPC, cancella tutte le regioni.
4. In Zone di disponibilità, scegli 3.

Best practice

- Elimina il VPC predefinito che viene fornito automaticamente in ogni nuovo account. Ciò impedisce agli utenti di avviare EC2 istanze pubbliche nell'account senza creare esplicitamente un VPC

dedicato. Per ulteriori informazioni, consulta la sezione Eliminazione delle sottoreti predefinite e del VPC predefinito (documentazione di Amazon Virtual Private Cloud). Puoi anche configurare AWS Control Tower Account Factory per Terraform (AFT) per eliminare automaticamente il VPC predefinito negli account appena creati.

- Effettua il provisioning di un nuovo dispositivo Account AWS chiamato dev-nonprod nell'unità organizzativa Workload >. NonProd Usa questo account per il tuo ambiente di sviluppo. Per istruzioni, vedere Provision Account Factory accounts with AWS Service Catalog (AWS Control Tower documentazione).

Definizione dei criteri di determinazione dell'ambito

Devi selezionare i criteri che la tua azienda utilizzerà per decidere se fornirne uno nuovo Account AWS. Puoi decidere di effettuare il provisioning degli account per ogni unità aziendale oppure decidere di eseguire il provisioning degli account in base all'ambiente, ad esempio produzione, test o controllo qualità. Ogni azienda ha i propri requisiti per quanto grande o piccola Account AWS dovrebbe essere. In genere, quando decidi come dimensionare i tuoi account, valuti i seguenti tre fattori:

- Bilanciamento delle quote di servizio: le quote di servizio sono i valori massimi per il numero di risorse, azioni e articoli per ciascuno Servizio AWS all'interno di un. Account AWS Se molti carichi di lavoro condividono lo stesso account e un carico di lavoro consuma la maggior parte o la totalità di una Service Quota, ciò potrebbe avere un impatto negativo su un altro carico di lavoro nello stesso account. In tal caso, potrebbe essere necessario separare tali carichi di lavoro in account diversi. Per ulteriori informazioni, consulta la sezione Servizio AWS Quotas (Riferimenti generali di AWS).
- Creazione di report sui costi: l'isolamento dei carichi di lavoro in account separati consente di visualizzare i costi a livello di account nei report sui costi e sull'utilizzo. Quando utilizzi lo stesso account per più carichi di lavoro, puoi utilizzare i tag per gestire e identificare le risorse. Per ulteriori informazioni sull'etichettatura, vedere Tagging resources (). AWSRiferimenti generali di AWS
- Controllo dell'accesso: quando i carichi di lavoro condividono un account, è necessario considerare come configurare le policy IAM per limitare l'accesso alle risorse dell'account in modo che gli utenti non abbiano accesso ai carichi di lavoro di cui non hanno bisogno. In alternativa, puoi utilizzare più account e set di autorizzazioni in Centro identità IAM per gestire l'accesso ai singoli account.

Best practice

- Rispetta le migliori pratiche in materia di strategia AWS multi-account per la tua AWS Control Tower landing zone (AWS Control Tower documentazione).
- Stabilisci una strategia di assegnazione dei tag efficace che ti aiuti a identificare e gestire le risorse AWS . È possibile utilizzare i tag per suddividere le risorse in categorie in base allo scopo, all'unità aziendale, all'ambiente o ad altri criteri. Per ulteriori informazioni, consulta Best practice for tagging (documentazione)Riferimenti generali di AWS .
- Non sovraccaricare un account con troppi carichi di lavoro. Se la richiesta del carico di lavoro supera una Service Quota, ciò può causare problemi di prestazioni. Puoi separare i carichi di lavoro concorrenti in diversi Account AWS oppure richiedere un aumento della quota di servizio. Per ulteriori informazioni, consulta la sezione Richiesta di aumento di una quota (documentazione Service Quotas).

Gestione delle autorizzazioni e dell'accesso per un'architettura multi-account

Questa sezione contiene gli argomenti seguenti:

- Considerazioni relative alla cultura ingegneristica
- Creazione di set di autorizzazioni
- Creazione di un limite delle autorizzazioni
- Gestione delle autorizzazioni per i singoli utenti

Considerazioni relative alla cultura ingegneristica

Uno dei pilastri del AWS Well-Architected Framework è l'eccellenza operativa. I team devono comprendere il modello operativo e il loro contributo al raggiungimento dei risultati aziendali. I team possono concentrarsi sul raggiungimento di obiettivi condivisi quando comprendono le proprie responsabilità, possono assumersi la titolarità e sapere come vengono prese le decisioni.

Nelle aziende in fase iniziale che si stanno sviluppando rapidamente, tutti i membri del team svolgono più ruoli. Non è raro che questi utenti abbiano un accesso altamente privilegiato all'intero Account AWS. Man mano che le aziende crescono, spesso vogliono seguire il principio di privilegio minimo e concedere solo le autorizzazioni necessarie all'utente per svolgere il proprio lavoro. Per aiutarti a limitare l'ambito, puoi utilizzare AWS Identity and Access Management Access Analyzer per vedere quali autorizzazioni utilizza effettivamente un utente o un ruolo IAM, che consente di rimuovere eventuali autorizzazioni in eccesso.

Può essere difficile decidere chi nella tua azienda dispone delle autorizzazioni per creare ruoli IAM. Si tratta in genere di un vettore per aumentare i privilegi. L'aumento dei privilegi si ha quando un utente può espandere le proprie autorizzazioni o l'ambito di accesso. Ad esempio, se un utente dispone di autorizzazioni limitate ma può creare nuovi ruoli IAM, può aumentare i propri privilegi creando e assumendo un nuovo ruolo IAM con la policy gestita `AdministratorAccess` applicata.

Alcune aziende limitano l'assegnazione dei ruoli IAM a un team centralizzato di persone fidate. L'aspetto negativo di questo approccio è che questo team può rapidamente diventare un ostacolo, perché quasi tutti Servizi AWS richiedono un ruolo IAM per funzionare. In alternativa, puoi usare i limiti delle autorizzazioni per delegare l'accesso IAM solo agli utenti che stanno sviluppando,

testando, lanciando e gestendo l'infrastruttura cloud. Ad esempio, consulta Example Permission Boundaries (). GitHub

I team addetti alle operazioni di sviluppo (DevOps), noti anche come team di piattaforma, spesso devono bilanciare le funzionalità self-service di più team di sviluppo interni con la stabilità operativa delle applicazioni. Promuovere una cultura ingegneristica che abbracci l'autonomia, la competenza e lo scopo sul posto di lavoro può aiutare a motivare i team. Gli ingegneri vogliono svolgere il proprio lavoro in modo autonomo, senza che gli altri debbano farle al posto loro. Se DevOps i team sono in grado di implementare soluzioni self-service, ciò riduce anche la quantità di tempo che gli altri dipendono da loro per portare a termine le proprie attività.

Creazione di set di autorizzazioni

È possibile gestire Account AWS l'accesso utilizzando i set di autorizzazioni in AWS IAM Identity Center. Un set di autorizzazioni è un modello che consente di implementare una o più policy IAM su più Account AWS. Quando si assegna un set di autorizzazioni a un Account AWS, il Centro identità IAM crea un ruolo IAM e associa le policy IAM a quel ruolo. Per ulteriori informazioni, consulta la sezione Creazione e gestione dei set di autorizzazioni (documentazione di Centro identità IAM).

AWS consiglia di creare set di autorizzazioni che corrispondano ai diversi personaggi dell'azienda.

A titolo di esempio si possono creare i set di autorizzazioni seguenti:

- Set di autorizzazioni di fatturazione
- Set di autorizzazioni per sviluppatori
- Set di autorizzazioni di produzione

I seguenti set di autorizzazioni sono frammenti di un modello. AWS CloudFormation È necessario utilizzare questo codice come punto di partenza e personalizzarlo per la propria attività. Per ulteriori informazioni sui CloudFormation modelli, consulta Learn template basics (documentazione). CloudFormation

Set di autorizzazioni di fatturazione

Il team finanziario lo utilizza BillingAccessPermissionSetper visualizzare la dashboard della AWS Billing console e AWS Cost Explorer in ogni account.

```
BillingAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
```

```
  Properties:
    Description: Access to Billing and Cost Explorer
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/Billing"
    Name: BillingAccess
    SessionDuration: PT8H
    RelayStateType: https://console.aws.amazon.com/billing/home
```

Set di autorizzazioni per sviluppatori

Il team di progettazione lo utilizza DeveloperAccessPermissionSetper accedere agli account non di produzione.

```
DeveloperAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to provision resources through CloudFormation
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:ContinueUpdateRollback",
              "cloudformation:CreateChangeSet",
              "cloudformation:CreateStack",
              "cloudformation:DeleteStack",
              "cloudformation:RollbackStack",
              "cloudformation:UpdateStack"
            ],
```

```
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              },
              "Null": {
                "cloudformation:ImportResourceTypes": true
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:CancelUpdateStack",
              "cloudformation:DeleteChangeSet",
              "cloudformation:DetectStackDrift",
              "cloudformation:DetectStackResourceDrift",
              "cloudformation:ExecuteChangeSet",
              "cloudformation:TagResource",
              "cloudformation:UntagResource",
              "cloudformation:UpdateTerminationProtection"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          },
          {
           "Effect": "Allow",
            "Action": [
              "cloudformation:CreateUploadBucket",
              "cloudformation:ValidateTemplate",
              "cloudformation:EstimateTemplateCost"
            ],
            "Resource": "*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSServiceCatalogEndUserFullAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSProtonDeveloperAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/ReadOnlyAccess"
    Name: DeveloperAccess
```

```
    SessionDuration: PT8H
```

Set di autorizzazioni di produzione

Il team di progettazione lo utilizza ProductionPermissionSetper accedere agli account di produzione. Questo set di autorizzazioni ha un accesso limitato e di sola visualizzazione.

```
ProductionPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to production accounts
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:ContinueUpdateRollback",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:CancelUpdateStack",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app-*"
          }
        ]
```

```
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/ViewOnlyAccess"
    Name: ProductionAccess
    SessionDuration: PT2H
```

Creazione di un limite delle autorizzazioni

Dopo aver distribuito i set di autorizzazioni, si stabilisce un limite delle autorizzazioni. Questo limite delle autorizzazioni è un meccanismo per delegare l'accesso IAM solo agli utenti che stanno sviluppando, testando, lanciando e gestendo l'infrastruttura cloud. Questi utenti possono eseguire solo le azioni consentite dalla policy e dal limite delle autorizzazioni.

È possibile definire il limite delle autorizzazioni in un AWS CloudFormation modello e quindi CloudFormation StackSets utilizzarlo per distribuire il modello in più account. Questo ti aiuta a stabilire e mantenere policy standardizzate in tutta l'organizzazione con un'unica operazione. Per ulteriori informazioni e istruzioni, vedete Lavorare con AWS CloudFormation StackSets (documentazione)CloudFormation .

Il seguente CloudFormation modello prevede un ruolo IAM e crea una policy IAM che funge da limite di autorizzazione. Utilizzando un set di stack, puoi implementare questo modello a tutti gli account membri della tua organizzazione.

```
CloudFormationRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        Effect: Allow
        Principal:
          Service: !Sub "cloudformation.${AWS::URLSuffix}"
        Action: "sts:AssumeRole"
        Condition:
          StringEquals:
            "aws:SourceAccount": !Ref "AWS::AccountId"
    Description: !Sub "DO NOT DELETE - Used by CloudFormation. Created by
 CloudFormation ${AWS::StackId}"
```

```
    ManagedPolicyArns:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess"
    PermissionsBoundary: !Ref DeveloperBoundary
    RoleName: CloudFormationRole

DeveloperBoundary:
  Type: "AWS::IAM::ManagedPolicy"
  Properties:
    Description: Permission boundary for developers
    ManagedPolicyName: PermissionsBoundary
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Sid: AllowModifyIamRolesWithBoundary
          Effect: Allow
          Action:
            - "iam:AttachRolePolicy"
            - "iam:CreateRole"
            - "iam:DeleteRolePolicy"
            - "iam:DetachRolePolicy"
            - "iam:PutRolePermissionsBoundary"
            - "iam:PutRolePolicy"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
          Condition:
            ArnEquals:
              "iam:PermissionsBoundary": !Sub "arn:${AWS::Partition}:iam::
${AWS::AccountId}:policy/PermissionsBoundary"
        - Sid: AllowModifyIamRoles
          Effect: Allow
          Action:
            - "iam:DeleteRole"
            - "iam:TagRole"
            - "iam:UntagRole"
            - "iam:UpdateAssumeRolePolicy"
            - "iam:UpdateRole"
            - "iam:UpdateRoleDescription"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
        - Sid: OverlyPermissiveAllowedServices
          Effect: Allow
          Action:
            - "lambda:*"
            - "apigateway:*"
            - "events:*"
            - "s3:*"
```

```
            - "logs:*"
          Resource: "*"
```

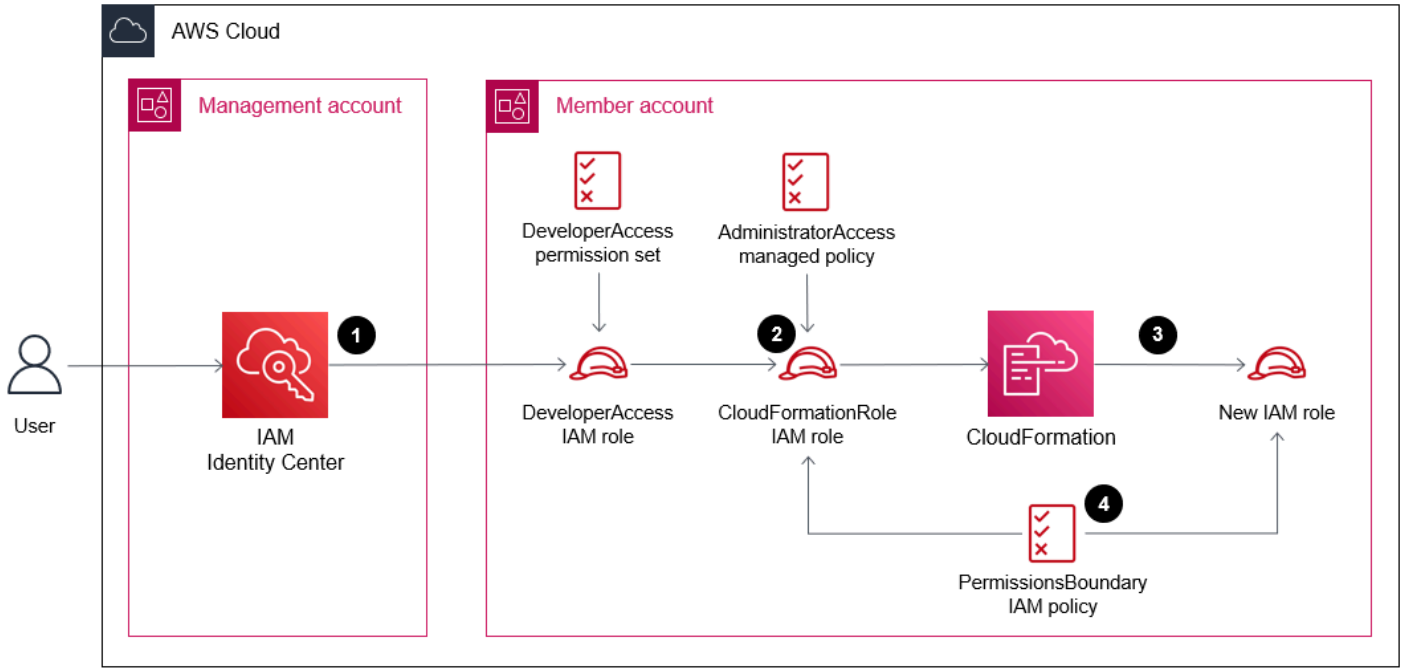
Il CloudFormationRoleruolo, la PermissionsBoundarypolicy e il set di DeveloperAccessautorizzazioni collaborano per concedere le seguenti autorizzazioni:

- Gli utenti hanno accesso in sola lettura alla maggior parte degli utenti Servizi AWS, tramite la ReadOnlyAccess AWS policy gestita.
- Gli utenti hanno accesso ai casi di supporto aperti, tramite la policy AWS gestita di AWSSupportaccesso.
- Gli utenti hanno accesso in sola lettura alla dashboard della AWS Billing console, tramite la policy AWSBillingReadOnlyAccess AWS gestita.
- Gli utenti possono effettuare il provisioning di nuovi ambienti da AWS Proton, tramite la policy AWSProtonDeveloperAccess AWS gestita.
- Gli utenti possono fornire prodotti da Service Catalog, tramite la policy AWSServiceCatalogEndUserFullAccess AWS gestita.
- Gli utenti sono in grado di convalidare e stimare il costo di qualsiasi CloudFormation modello, tramite la politica in linea.
- Utilizzando il ruolo CloudFormationRoleIAM, gli utenti possono creare, aggiornare o eliminare qualsiasi CloudFormation stack che inizia con app/.
- Gli utenti possono utilizzare per CloudFormation creare, aggiornare o eliminare i ruoli IAM che iniziano con app/. La policy PermissionsBoundaryIAM impedisce agli utenti di aumentare i propri privilegi.
- Gli utenti possono effettuare il provisioning di risorse Amazon AWS Lambda EventBridge CloudWatch, Amazon, Amazon Simple Storage Service (Amazon S3) e Amazon API Gateway solo utilizzando. CloudFormation

L'immagine seguente mostra come un utente autorizzato, ad esempio uno sviluppatore, può creare un nuovo ruolo IAM in un account membro utilizzando i set di autorizzazioni, i ruoli IAM e i limiti delle autorizzazioni descritti in questa guida:

1. L'utente si autentica in IAM Identity Center e assume il ruolo IAM. DeveloperAccess
2. L'utente avvia l'`cloudformation:CreateStack`azione e assume il ruolo IAM. CloudFormationRole

3. L'utente avvia l'`iam:CreateRole`azione e la utilizza CloudFormation per creare un nuovo ruolo IAM.
4. La policy PermissionsBoundaryIAM viene applicata al nuovo ruolo IAM.



Al CloudFormationRoleruolo è associata la policy AdministratorAccessgestita, ma grazie alla policy PermissionsBoundaryIAM, le autorizzazioni effettive del CloudFormationRoleruolo diventano uguali alla PermissionsBoundarypolicy. La PermissionsBoundarypolicy fa riferimento a se stessa quando consente l'`iam:CreateRole`azione, il che garantisce che i ruoli possano essere creati solo se viene applicato il limite delle autorizzazioni.

Gestione delle autorizzazioni per i singoli utenti

Utilizzando i set di autorizzazioni, il limite delle autorizzazioni e il ruolo CloudFormationRoleIAM, puoi limitare la quantità di autorizzazioni che devi assegnare direttamente ai singoli responsabili. In questo modo puoi gestire l'accesso man mano che l'azienda cresce e applicare le best practice di sicurezza di concessione del privilegio minimo.

Puoi anche usare ruoli collegati ai servizi, che concedono le autorizzazioni a un servizio AWS di eseguire il provisioning delle risorse per tuo conto. Invece di concedere le autorizzazioni al principale IAM (utente, gruppo di utenti o ruolo), puoi concedere le autorizzazioni al servizio. A titolo di esempio si possono menzionare i ruoli collegati al servizio per AWS Proton e AWS Service Catalog

ti consentono di eseguire il provisioning di modelli, risorse e ambienti personalizzati, senza assegnare autorizzazioni al principale IAM. Per ulteriori informazioni, consulta la sezione Servizi AWS che funzionano con IAM e Utilizzo di ruoli collegati ai servizi (documentazione IAM).

Un'altra best practice consiste nel limitare la quantità di accesso degli individui alla AWS Management Console. Limitando l'accesso alla console, puoi richiedere agli utenti di fornire risorse utilizzando tecnologie Infrastructure as Code (IaC), come Terraform o Pulumi. AWS CloudFormationHashiCorp Gestendo l'infrastruttura tramite IAc è possibile tenere traccia delle modifiche alle risorse nel tempo e introdurre meccanismi per l'approvazione delle modifiche, come le pull request. GitHub

Connettività di rete per un'architettura multi-account

Connessione VPCs

Molte aziende utilizzano il peering VPC in Amazon Virtual Private Cloud (Amazon VPC) per collegare sviluppo e produzione. VPCs Utilizzando una connessione peering VPC, puoi instradare il traffico tra due VPCs utilizzando l'indirizzamento IP privato. Il connesso VPCs può essere in diversi Account AWS e in diversi. Regioni AWS Per ulteriori informazioni, consulta la sezione Che cos'è il peering VPC? (documentazione di Amazon VPC). Man mano che le aziende crescono e il numero di aziende VPCs aumenta, mantenere connessioni peering tra tutte VPCs può diventare un onere di manutenzione. Potresti anche incorrere nei limiti previsti dal numero massimo di connessioni peering VPC per VPC. Per ulteriori informazioni, consulta la sezione Quota di connessione peering VPC (documentazione di Amazon VPC).

Se disponi di più ambienti di sviluppo, test e gestione temporanea che ospitano dati non di produzione su più ambienti Account AWS, potresti voler fornire la connettività di rete tra tutti questi ambienti VPCs ma impedire l'accesso agli ambienti di produzione. È possibile utilizzarlo AWS Transit Gatewayper connettere più account VPCs . È possibile separare le tabelle di routing per evitare che lo sviluppo VPCs comunichi con la produzione VPCs attraverso il gateway di transito, che funge da router centralizzato. Per ulteriori informazioni, consulta la sezione Router centralizzato (documentazione Transit Gateway).

Transit Gateway supporta anche il peering con altri gateway di transito, inclusi quelli in diversi Account AWS o Regioni AWS. Poiché Transit Gateway è un servizio completamente gestito e ad alta disponibilità, è necessario fornire un solo gateway di transito per ogni regione.

Per ulteriori informazioni e architetture di rete dettagliate, vedere Creazione di un'infrastruttura di AWS rete multi-VPC scalabile e sicura (Whitepaper).AWS

Connessione di applicazioni

Se è necessario stabilire una comunicazione tra applicazioni diverse nello stesso ambiente (ad esempio Account AWS in produzione), è possibile utilizzare una delle seguenti opzioni:

- Peering VPC o AWS Transit Gateway può offrire connettività a livello di rete se desideri aprire un ampio accesso a più indirizzi IP e porte.

- AWS PrivateLink crea endpoint in una sottorete privata del VPC e questi endpoint vengono registrati come voci DNS in Amazon Route 53 Resolver. Utilizzando il DNS, le applicazioni possono risolvere gli endpoint e connettersi ai servizi registrati, senza richiedere gateway NAT o gateway Internet nel VPC.
- Amazon VPC Lattice associa servizi, come le applicazioni, su più account VPCs e li raccoglie in una rete di servizi. I client VPCs associati alla rete di servizi possono inviare richieste a tutti gli altri servizi associati alla rete di servizi, indipendentemente dal fatto che si trovino nello stesso account. VPC Lattice si integra con AWS Resource Access Manager (AWS RAM) in modo da poter condividere le risorse con altri account o tramite. AWS Organizations Puoi associare un VPC a una sola rete di servizi. Questa soluzione non richiede l'uso del peering VPC o AWS Transit Gateway per comunicare tra account.

Best practice per la connettività di rete

- Creane uno Account AWS da utilizzare per la rete centralizzata. Assegna un nome a questo account network-prod e utilizzalo per AWS Transit Gateway Amazon VPC IP Address Manager (IPAM). Aggiungi questo account all'unità organizzativa Infrastructure_Prod.
- Usa AWS Resource Access Manager (AWS RAM) per condividere il gateway di transito, le reti di servizi VPC Lattice e i pool IPAM con il resto dell'organizzazione. Ciò consente a chiunque Account AWS all'interno dell'organizzazione di interagire con questi servizi.
- Utilizzando i pool IPAM per gestire IPv4 e IPv6 indirizzare centralmente le allocazioni, è possibile consentire agli utenti finali di eseguire autonomamente l'approvvigionamento utilizzando. VPCs AWS Service Catalog Ciò consente di dimensionare in modo appropriato VPCs e prevenire la sovrapposizione degli spazi di indirizzi IP.
- Utilizza un approccio centralizzato in uscita per il traffico diretto a Internet e utilizza un approccio di ingresso decentralizzato per il traffico proveniente dal tuo ambiente da Internet. Per ulteriori informazioni, consulta Uscita centralizzata e Ingresso decentralizzato.

Uscita centralizzata

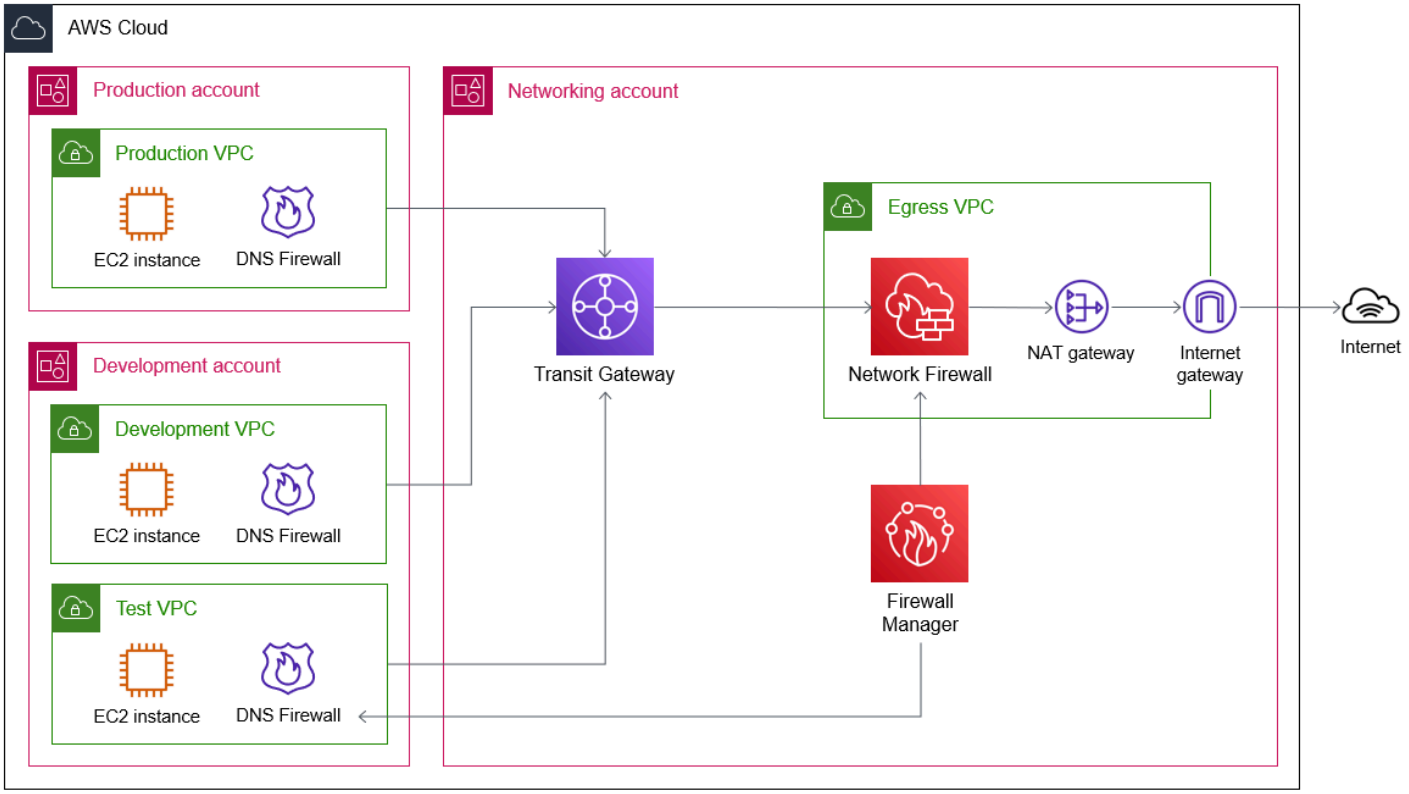
Uscita centralizzata è il principio dell'utilizzo di un unico punto di ispezione comune per tutto il traffico di rete destinato a Internet. In questo punto di ispezione, puoi consentire il traffico solo verso domini specifici o solo attraverso porte o protocolli specifici. La centralizzazione delle uscite può inoltre aiutarvi a ridurre i costi eliminando la necessità di implementare gateway NAT in ognuno di voi per accedere a Internet. VPCs Ciò è vantaggioso dal punto di vista della sicurezza perché limita

l'esposizione a risorse dannose accessibili dall'esterno, come l'infrastruttura di comando e controllo (C&C) del malware. Per ulteriori informazioni e opzioni di architettura per l'uscita centralizzata, consulta la sezione Uscita centralizzata verso Internet (white paper).AWS

Puoi utilizzare AWS Network Firewall, che è un firewall di rete stateful e gestito e un servizio di rilevamento e prevenzione delle intrusioni, che funge da punto di ispezione centrale per il traffico in uscita. È necessario configurare questo firewall in un VPC dedicato per il traffico in uscita. Firewall di rete supporta regole stateful che puoi utilizzare per limitare l'accesso a Internet a domini specifici. Per ulteriori informazioni, consulta la sezione Domain List (documentazione Firewall di rete).

Puoi anche utilizzare Firewall DNS Amazon Route 53 Resolver per limitare il traffico in uscita verso nomi di dominio specifici, principalmente per impedire l'esfiltrazione non autorizzata dei dati. Nelle regole di Firewall DNS, puoi applicare elenchi di domini (documentazione Route 53), che consentono o negano l'accesso a domini specifici. È possibile utilizzare elenchi di domini AWS gestiti, che contengono nomi di dominio associati ad attività dannose o altre potenziali minacce, oppure creare elenchi di domini personalizzati. Crei gruppi di regole del firewall DNS e poi li applichi ai tuoi VPCs. Le richieste DNS in uscita vengono instradate attraverso un Resolver nel VPC per la risoluzione dei nomi di dominio e Firewall DNS filtra le richieste in base ai gruppi di regole applicati al VPC. Le richieste DNS ricorsive che vanno al Resolver non fluiscono attraverso il gateway di transito e il percorso di Firewall di rete. Route 53 Resolver e Firewall DNS devono essere considerati un percorso di uscita separato dal VPC.

L'immagine seguente mostra un'architettura di esempio per l'uscita centralizzata. Prima che inizi la comunicazione di rete, le richieste DNS vengono inviate al Route 53 Resolver, dove il firewall DNS consente o nega la risoluzione dell'indirizzo IP utilizzato per la comunicazione. Il traffico destinato a Internet viene indirizzato a un gateway di transito in un account di rete centralizzato. Il gateway di transito inoltra il traffico a Firewall di rete per l'ispezione. Se la policy del firewall consente il traffico in uscita, il traffico viene indirizzato attraverso un gateway NAT, attraverso un gateway Internet e verso Internet. Puoi utilizzarlo AWS Firewall Manager per gestire centralmente i gruppi di regole del firewall DNS e le politiche del Network Firewall nell'infrastruttura multi-account.



Best practice per proteggere il traffico in uscita

- Inizia in modalità di sola registrazione (documentazione Route 53). Passa alla modalità di blocco dopo aver verificato che il traffico legittimo non è interessato.
- Blocca il traffico DNS diretto a Internet utilizzando AWS Firewall Manager le politiche per gli elenchi di controllo degli accessi alla rete o utilizzando. AWS Network Firewall Tutte le query DNS devono essere instradate attraverso un Route 53 Resolver, dove puoi monitorarle con Amazon GuardDuty (se abilitato) e filtrarle con Route 53 Resolver DNS Firewall (se abilitato). Per ulteriori informazioni, consulta Risoluzione delle query DNS tra e la rete (documentazione di Route 53). VPCs
- Utilizza gli Elenchi di domini gestiti da AWS(documentazione Route 53) in Firewall DNS e Firewall di rete.
- Valuta la possibilità di bloccare i domini di primo livello inutilizzati e ad alto rischio, come .info, .top, .xyz o alcuni domini con codice paese.
- Valuta la possibilità di bloccare le porte non utilizzate e ad alto rischio, come le porte 1389, 4444, 3333, 445, 135, 139 o 53.
- Come punto di partenza, puoi utilizzare un elenco di negazioni che include le regole gestite. AWS È quindi possibile passare il tempo all'implementazione di un modello di elenco di autorizzazioni.

Ad esempio, invece di includere solo un elenco ristretto di nomi di dominio completi nell'elenco consentito, inizia utilizzando alcuni caratteri jolly, come *.example.com. Puoi anche consentire solo i domini di primo livello che ti aspetti e bloccare tutti gli altri. Poi, col tempo, restringi anche quelli.

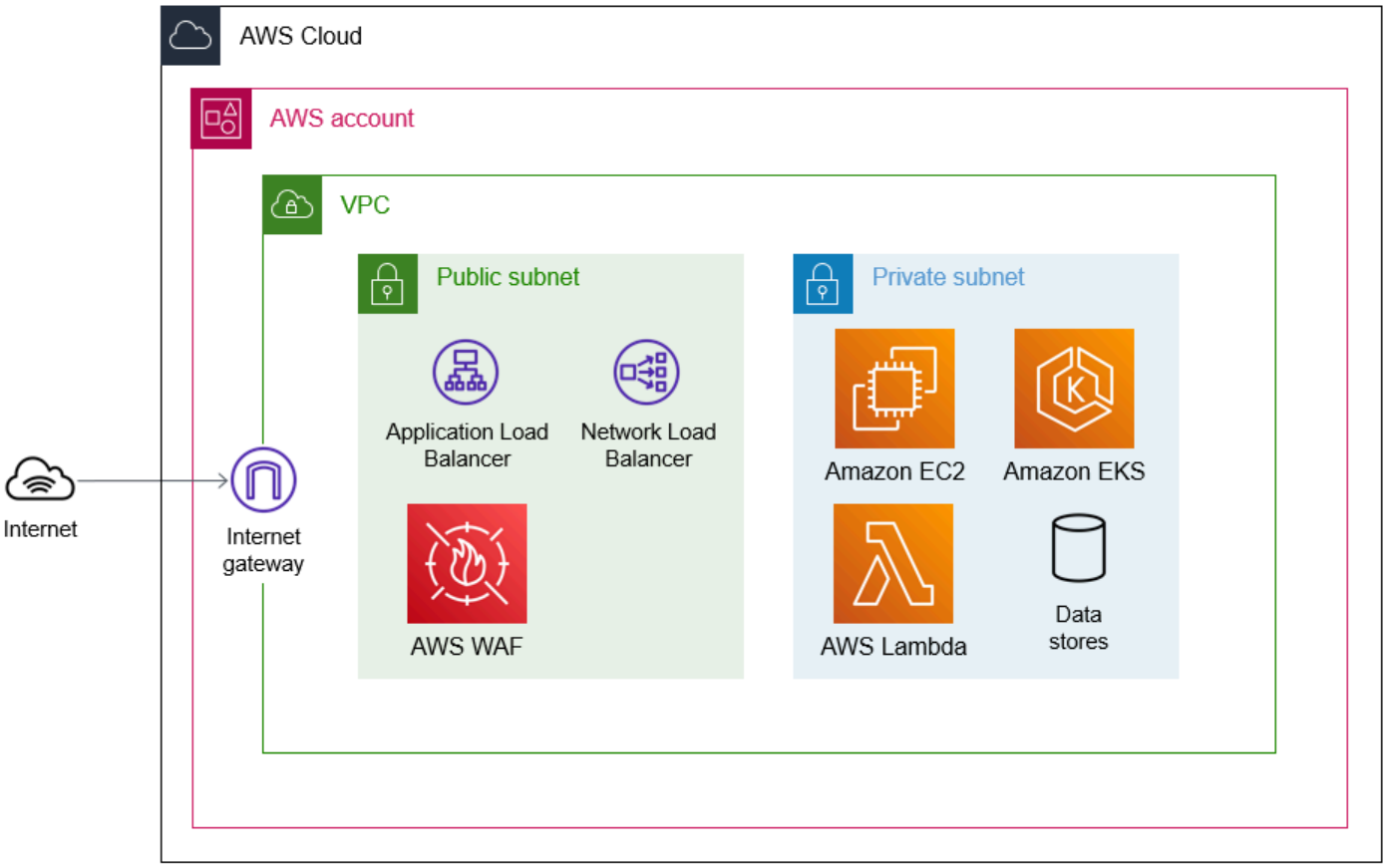
- Usa i profili Route 53 (documentazione Route 53) per applicare le configurazioni Route 53 relative al DNS a molte configurazioni Route 53 VPCs e in diversi modi. Account AWS
- Definisci un processo per la gestione delle eccezioni a queste best practice.

Ingresso decentralizzato

Ingresso decentralizzato è un principio per definire, a livello di singolo account, in che modo il traffico proveniente da Internet raggiunge i carichi di lavoro di quell'account. Nelle architetture multi-account, uno dei vantaggi dell'ingresso decentralizzato è che ogni account può utilizzare il servizio o la risorsa di ingresso più appropriati per i propri carichi di lavoro, come Application Load Balancer, Gateway Amazon API o Network Load Balancer.

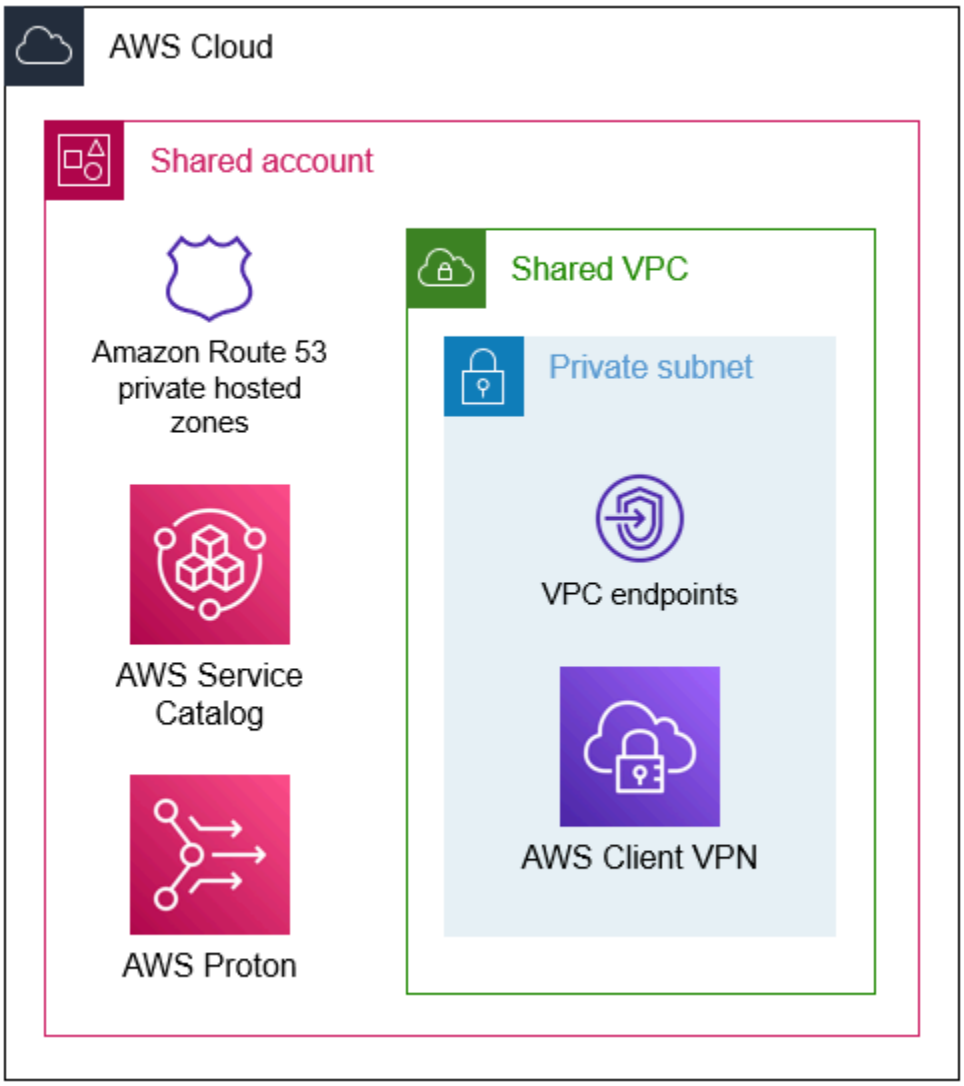
Sebbene l'accesso decentralizzato implichi la necessità di gestire ogni account singolarmente, è possibile amministrare e mantenere centralmente le configurazioni tramite AWS Firewall Manager. Firewall Manager supporta protezioni come AWS WAF e Gruppi di sicurezza Amazon VPC. Puoi associarti AWS WAF a un Application Load Balancer CloudFront, Amazon, API Gateway o. AWS AppSync Se utilizzi un VPC di uscita e un gateway di transito, come descritto in Uscita centralizzata, ogni VPC spostato contiene sottoreti pubbliche e private. Tuttavia, non è necessario implementare gateway NAT poiché il traffico viene indirizzato attraverso il VPC di uscita nell'account di rete.

L'immagine seguente mostra un esempio di un individuo Account AWS che dispone di un singolo VPC contenente un carico di lavoro accessibile da Internet. Il traffico proveniente da Internet accede al VPC tramite un gateway Internet e raggiunge i servizi di bilanciamento del carico e di sicurezza ospitati in una sottorete pubblica. (Una sottorete pubblica contiene una route predefinita a un gateway Internet). Implementa i sistemi di bilanciamento del carico nelle sottoreti pubbliche e allega gli elenchi di controllo degli AWS WAF accessi (ACLs) per proteggerti dal traffico dannoso, come lo scripting tra siti. Implementa carichi di lavoro che ospitano le applicazioni in sottoreti private, che non hanno accesso diretto da e verso Internet.



Se VPCs nella tua organizzazione ne hai molti, potresti voler condividere qualcosa in comune Servizi AWS creando endpoint VPC di interfaccia o zone private ospitate in un ambiente dedicato e condiviso. Account AWS Per ulteriori informazioni, consulta Accedere a un endpoint VPC Servizio AWS con interfaccia (AWS PrivateLink documentazione) e Lavorare con zone ospitate private (documentazione Route 53).

L'immagine seguente mostra un esempio di un ambiente Account AWS che ospita risorse che possono essere condivise all'interno dell'organizzazione. Gli endpoint VPC possono essere condivisi tra più account creandoli in un VPC dedicato. Quando crei un endpoint VPC, puoi facoltativamente far gestire ad AWS le voci DNS per l'endpoint. Per condividere un endpoint, deseleziona questa opzione e crea le voci DNS in una zona ospitata privata (PHZ) separata di Route 53. È quindi possibile associare il PHZ a tutti i componenti dell' VPCs organizzazione per la risoluzione DNS centralizzata degli endpoint VPC. È inoltre necessario assicurarsi che le tabelle delle rotte del gateway di transito includano le rotte tra il VPC condiviso e l'altro. VPCs Per ulteriori informazioni, consulta Accesso centralizzato agli endpoint VPC di interfaccia (Whitepaper)AWS .



Un ambiente condiviso Account AWS è anche un buon posto per ospitare portafogli. AWS Service Catalog Un portfolio è una raccolta di servizi IT che si desidera rendere disponibili per l'implementazione e il portafoglio contiene informazioni di configurazione per tali servizi. AWSÈ possibile creare i portafogli nell'account condiviso, condividerli con l'organizzazione, quindi ogni account membro importa il portafoglio nella propria istanza regionale del Service Catalog. Per ulteriori informazioni, consulta la sezione Condivisione con AWS Organizations (documentazione Service Catalog).

Analogamente, con AWS Proton, è possibile utilizzare l'account condiviso per gestire centralmente l'ambiente e i modelli di servizio e quindi configurare le connessioni degli account con gli account dei membri dell'organizzazione. Per ulteriori informazioni, consulta Environment account connections (AWS Proton documentazione).

Risposta agli incidenti di sicurezza per un'architettura multi-account

Durante la transizione a più sistemi Account AWS, è importante mantenere la visibilità sugli eventi di sicurezza che potrebbero verificarsi all'interno dell'organizzazione. In Gestione delle identità e controllo degli accessi, hai usato AWS Control Tower per configurare la tua zona di destinazione. Durante il processo di configurazione, ho AWS Control Tower designato un pulsante Account AWS per la sicurezza. È necessario delegare l'amministrazione dei servizi di sicurezza all'security-tooling-prodaccount e utilizzare questo account per gestire centralmente questi servizi.

Questa guida esamina l'uso di quanto segue Servizi AWS per proteggere l'utente Account AWS e l'organizzazione:

- Amazon GuardDuty
- Amazon Macie
- AWS Security Hub

Amazon GuardDuty

Amazon GuardDuty è un servizio di monitoraggio continuo della sicurezza che analizza le fonti di dati, come i registri AWS CloudTrail degli eventi. Per un elenco completo delle fonti di dati supportate, consulta Come Amazon GuardDuty utilizza le sue fonti di dati (GuardDuty documentazione). Utilizza feed di intelligence di minacce, come elenchi di domini e di IP dannosi nonché il machine learning per identificare attività inattese e potenzialmente non autorizzate e dannose nell'ambiente AWS .

Quando utilizzi GuardDuty with AWS Organizations, l'account di gestione dell'organizzazione può designare qualsiasi account dell'organizzazione come amministratore GuardDuty delegato. L'amministratore delegato diventa l'account GuardDuty amministratore per la regione. GuardDuty viene abilitato automaticamente in questo:Regione AWS e l'account amministratore delegato dispone delle autorizzazioni GuardDuty per abilitare e gestire tutti gli account dell'organizzazione all'interno di quella regione. Per ulteriori informazioni, vedere Gestire GuardDuty gli account con AWS Organizations (GuardDuty documentazione).

GuardDuty è un servizio regionale. Ciò significa che è necessario abilitarlo GuardDuty in ogni regione che si desidera monitorare.

Best practice

- Abilita GuardDuty in tutte le versioni supportate Regioni AWS. GuardDuty può generare informazioni su attività non autorizzate o insolite, anche in Regioni che non utilizzi attivamente. I prezzi GuardDuty si basano sul numero di eventi analizzati. Anche nelle regioni in cui non si gestiscono carichi di lavoro, l'abilitazione GuardDuty è uno strumento di rilevamento efficace ed economico per avvisare l'utente in caso di attività potenzialmente dannose. Per ulteriori informazioni sulle regioni in cui GuardDuty è disponibile, consulta Amazon GuardDuty service endpoints (Riferimenti generali di AWS).
- In ogni regione, delega l'security-tooling-prodaccount da amministrare GuardDuty per la tua organizzazione. Per ulteriori informazioni, vedere Designazione di un amministratore GuardDuty delegato (documentazione). GuardDuty
- Configura GuardDuty per iscrivere automaticamente i nuovi non Account AWS appena vengono aggiunti all'organizzazione. Per ulteriori informazioni, consulta la Fase 3: automatizzare l'aggiunta di nuovi account dell'organizzazione come membri in Gestire gli account con AWS Organizations (GuardDuty documentazione).

Amazon Macie

Amazon Macie è un servizio di sicurezza e privacy dei dati completamente gestito che utilizza il machine learning e la corrispondenza di modelli per individuare, monitorare e aiutare a proteggere i dati sensibili in Amazon Simple Storage Service (Amazon S3). Puoi esportare dati da Amazon Relational Database Service (Amazon RDS) e Amazon DynamoDB in un bucket S3 e quindi utilizzare Macie per scansionare i dati.

Quando usi Macie con AWS Organizations, l'account di gestione dell'organizzazione può designare qualsiasi account dell'organizzazione come account amministratore di Macie. L'account amministratore può abilitare e gestire Macie per gli account dei membri dell'organizzazione, può accedere ai dati dell'inventario Amazon S3 ed eseguire processi di rilevamento di dati sensibili per gli account. Per ulteriori informazioni, consulta la sezione Gestione degli account con AWS Organizations (documentazione Macie).

Macie è un servizio regionale. Ciò significa che è necessario abilitare Macie in ogni regione che si desidera monitorare e che l'account amministratore Macie può gestire gli account dei membri solo all'interno della stessa regione.

Best practice

- Aderisci alle Considerazioni e consigli per l'utilizzo di Macie con AWS Organizations (documentazione Macie).
- In ogni regione, delega l'security-tooling-prodaccount per amministrare Macie per la tua organizzazione. Per gestire centralmente più account Macie Regioni AWS, l'account di gestione deve accedere a ciascuna regione in cui l'organizzazione utilizza attualmente o utilizzerà Macie e quindi designare l'account amministratore Macie in ciascuna di tali regioni. L'account amministratore Macie può quindi configurare l'organizzazione in ciascuna di queste regioni. Per ulteriori informazioni, consulta la sezione Integrazione e configurazione di un'organizzazione (documentazione Macie).
- Macie offre un piano gratuito mensile per i lavori di rilevamento di dati sensibili. Se hai dati sensibili archiviati in Amazon S3, usa Macie per analizzare i tuoi bucket S3 come parte del piano gratuito mensile. Se superi il limite previsto dal piano gratuito, per il tuo account cominceranno a incorrere i costi per l'individuazione di dati sensibili.

AWS Security Hub

AWS Security Hubti offre una visione completa del tuo stato di sicurezza in. AWS Puoi utilizzarlo per verificare l'ambiente rispetto agli standard e alle best practice del settore della sicurezza. Security Hub raccoglie dati sulla sicurezza da tutti i tuoi Account AWS servizi (incluso Macie) GuardDuty e dai prodotti partner di terze parti supportati. Security Hub ti aiuta ad analizzare le tendenze di sicurezza e identificare i problemi di sicurezza più importanti. Security Hub fornisce diversi standard di sicurezza che puoi abilitare per eseguire controlli di conformità in ciascun Account AWS.

Quando si utilizza Security Hub con AWS Organizations, l'account di gestione dell'organizzazione può designare qualsiasi account dell'organizzazione come account amministratore di Security Hub. L'account amministratore di Security Hub può quindi abilitare e gestire gli account di altri membri dell'organizzazione. Per ulteriori informazioni, vedere Utilizzo AWS Organizations per gestire gli account (documentazione del Security Hub).

Security Hub è un servizio regionale. Ciò significa che è necessario abilitare Security Hub in ogni regione che si desidera analizzare e in AWS Organizations, è necessario definire l'amministratore delegato per ogni regione.

Best practice

- Aderisci ai Prerequisiti e consigli (documentazione Security Hub).
- In ogni regione, delega l'security-tooling-prodaccount all'amministrazione del Security Hub per la tua organizzazione. Per ulteriori informazioni, consulta la sezione Designazione di un account amministratore di Security Hub (documentazione Security Hub).
- Configura Security Hub per registrarne automaticamente di nuovi Account AWS quando vengono aggiunti all'organizzazione.
- Abilita lo Standard AWS Foundational Security Best Practices (documentazione Security Hub) per rilevare quando le risorse si discostano dalle best practice di sicurezza.
- Abilita lo Strumento di aggregazione multiregionale (documentazione Security Hub) in modo da poter visualizzare e gestire tutti i risultati del Security Hub da un'unica regione.

Configurazione dei backup per un'architettura multi-account

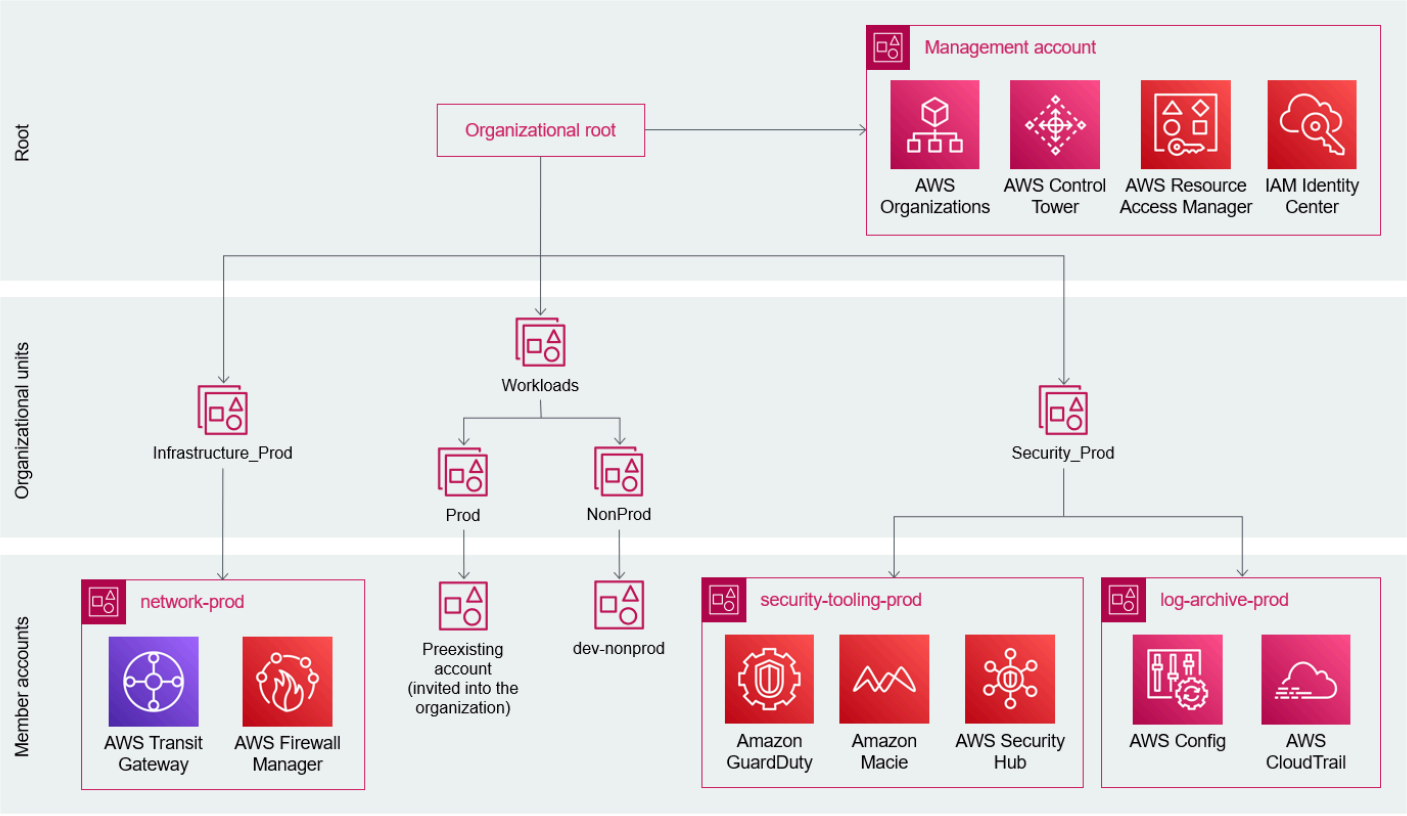
Una strategia di backup completa è una parte essenziale del piano di protezione dei dati di un'azienda per resistere a qualsiasi impatto, recuperare e ridurre qualsiasi rischio di impatto che potrebbe avvenire a causa di un evento di sicurezza. Una policy di backup ti consente di standardizzare e implementare una strategia di backup per le risorse in tutti gli account dell'organizzazione. In una policy di backup, è possibile configurare e distribuire piani di backup per le risorse. Per ulteriori informazioni, vedere Politiche di Backup (AWS Organizations documentazione). Per ulteriori informazioni, consulta le 10 migliori pratiche di sicurezza per proteggere i backup in AWS (AWS Prescriptive Guidance).

Migrazione nell'account durante la transizione a un'architettura multi-account

In Invita il tuo account preesistente, hai invitato il tuo account preesistente a partecipare all'unità organizzativa Carichi di lavoro > Prod. Questo account è ora gestito come parte dell'organizzazione.

Hai inoltre effettuato il provisioning di un nuovo account dev-nonprod nell'unità organizzativa Workload >. NonProd I membri del team dovrebbero ora essere in grado di accedere agli account appropriati tramite. AWS IAM Identity Center Rimuovi tutti i singoli account utente in AWS Identity and Access Management (IAM).

Se hai seguito i consigli di questa guida, la tua organizzazione ha ora la seguente struttura.



Se ci sono carichi di lavoro in esecuzione all'interno dell'account preesistente, ora esegui la migrazione di questi carichi di lavoro in account indipendenti, in base ai criteri stabiliti in Definizione dei criteri di determinazione dell'ambito. Esegui la migrazione di tutti i carichi di lavoro non di produzione alla nuova unità organizzativa dev-nonprod ed esegui la migrazione dei carichi di lavoro

di produzione all'account network-prod. Per ulteriori informazioni sulla migrazione AWS delle risorse comuni, consulta la sezione seguente di questa guida,. Migrazione delle risorse

Replica o migrazione delle risorse tra Account AWS

Dopo la migrazione da un'architettura a account singolo Account AWS a quella con più account, è normale che carichi di lavoro di produzione e non di produzione vengano eseguiti nell'account preesistente. La migrazione di queste risorse verso account o unità organizzative di produzione e non di produzione dedicati consente di gestire l'accesso e il networking per questi carichi di lavoro. Di seguito sono riportate alcune opzioni per la migrazione di risorse comuni in un'altra. AWS Account AWS

Questa sezione si concentra sulle strategie per la replica dei dati tra Account AWS. È necessario fare in modo che i carichi di lavoro siano il più possibile stateless per evitare di dover replicare le risorse di elaborazione tra account. È inoltre utile gestire le risorse tramite Infrastruttura come codice (IaC) in modo da poter rifornire un ambiente in un Account AWS separato.

Questa sezione esamina le opzioni per la migrazione delle seguenti risorse di dati:

- AWS AppConfig configurazioni e ambienti
- AWS Certificate Manager certificati
- CloudFront Distribuzioni Amazon
- AWS CodeArtifact domini e repository
- Tabelle Amazon DynamoDB
- Volumi Amazon EBS
- EC2 Istanze Amazon o AMIs
- Registri Amazon ECR
- File system di Amazon EFS
- Cluster Amazon ElastiCache (Redis OSS)
- AWS Elastic Beanstalk ambienti
- Indirizzi IP elastici
- AWS Lambda livelli
- Istanze Amazon Lightsail
- Cluster Amazon Neptune
- Domini Amazon OpenSearch Service
- Snapshot di Amazon RDS
- Cluster Amazon Redshift

- Domini e zone ospitate di Amazon Route 53
- Bucket Amazon S3
- Modelli Amazon SageMaker AI
- AWS WAF web ACLs

AWS AppConfig configurazioni e ambienti

AWS AppConfig non supporta la copia diretta della sua configurazione su un'altra. Account AWS Tuttavia, è consigliabile gestire AWS AppConfig le configurazioni e gli ambienti separatamente da quelli Account AWS che li ospitano. Per ulteriori informazioni, consulta Configurazione tra account con AWS AppConfig (post AWS del blog).

AWS Certificate Manager certificati

Non è possibile esportare direttamente un certificato AWS Certificate Manager (ACM) da un account a un altro perché la chiave AWS Key Management Service (AWS KMS) utilizzata per crittografare la chiave privata del certificato è unica per ogni Regione AWS account. Tuttavia, puoi fornire contemporaneamente più certificati con lo stesso nome di dominio su più account e regioni. ACM supporta la convalida della proprietà del dominio tramite DNS (consigliato) o e-mail. Quando utilizzi la convalida DNS e crei un nuovo certificato, ACM genera un record CNAME univoco per ogni dominio del certificato. Il record CNAME è unico per ogni account e deve essere aggiunto alla zona ospitata di Amazon Route 53 o al provider DNS entro 72 ore affinché il certificato venga convalidato correttamente.

CloudFront Distribuzioni Amazon

Amazon CloudFront non supporta la migrazione delle distribuzioni da una Account AWS all'altra Account AWS. Tuttavia, CloudFront supporta la migrazione di un nome di dominio alternativo, noto anche come CNAME, da una distribuzione all'altra. Per ulteriori informazioni, consulta Come posso risolvere l'errore CNAMEAlready Exists quando configuro un alias CNAME per la mia CloudFront distribuzione (AWS Knowledge Center).

AWS CodeArtifact domini e repository

Sebbene un'organizzazione possa avere più domini, ti consigliamo di disporre di un unico dominio di produzione che contenga tutti gli artefatti pubblicati. Questo aiuta i team di sviluppo a trovare

e condividere i pacchetti all'interno dell'organizzazione. Il Account AWS proprietario del dominio può essere diverso dall'account che possiede gli eventuali repository associati al dominio. È possibile copiare pacchetti tra repository, ma devono appartenere allo stesso dominio. Per ulteriori informazioni, consulta Copiare i pacchetti tra i repository (CodeArtifact documentazione).

Tabelle Amazon DynamoDB

Puoi utilizzare uno dei seguenti servizi per eseguire la migrazione di una tabella Amazon DynamoDB verso un altro Account AWS:

- AWS Backup
- Importazione ed esportazione da DynamoDB ad Amazon S3
- Amazon S3 e AWS Glue
- AWS Data Pipeline
- Amazon EMR

Per ulteriori informazioni, consulta Come posso migrare le mie tabelle Amazon DynamoDB Account AWS da una all'AWS altra (Knowledge Center).

Volumi Amazon EBS

Puoi acquisire uno snapshot di un volume Amazon Elastic Block Store (Amazon EBS) esistente, condividere lo snapshot con l'account di destinazione e crearne una copia nell'account di destinazione. In questo modo migra in modo efficace il volume da un account all'altro. Per ulteriori informazioni, consulta Come posso condividere uno snapshot o un volume Amazon EBS crittografato con un altro Account AWS (AWS Knowledge Center).

EC2 Istanze Amazon o AMIs

Non è possibile trasferire direttamente istanze Amazon Elastic Compute Cloud (Amazon EC2) o Amazon Machine Images (AMIs) esistenti su un altro. Account AWS Puoi invece creare un'AMI personalizzata nell'account di origine, condividere l'AMI con l'account di destinazione, avviare una nuova EC2 istanza dall'AMI condivisa nell'account di destinazione, quindi annullare la registrazione dell'AMI condivisa.

Registri Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) supporta la replica tra account e tra regioni. Puoi configurare la replica nel registro di origine e una policy di autorizzazione del registro nel registro di destinazione. Per ulteriori informazioni, consulta la sezione Configurazione della replica tra account (documentazione Amazon ECR) e Consentire all'utente root di un account di origine di replicare tutti i repository (documentazione Amazon ECR).

File system di Amazon EFS

Amazon Elastic File System (Amazon EFS) supporta la replica tra account e regioni. È possibile configurare la replica sul file system di origine. Per ulteriori informazioni, consulta Replicating file system (documentazione Amazon EFS).

Cluster Amazon ElastiCache (Redis OSS)

Puoi utilizzare un backup di un cluster di database Amazon ElastiCache (Redis OSS) per migrarlo su un altro account. Per ulteriori informazioni, consulta Quali sono le migliori pratiche per la migrazione del mio cluster ElastiCache (Redis OSS) (AWS Knowledge Center).

AWS Elastic Beanstalk ambienti

Infatti AWS Elastic Beanstalk, puoi utilizzare le configurazioni salvate (documentazione di Elastic Beanstalk) per migrare un ambiente in un altro. Account AWS Per ulteriori informazioni, consulta Come faccio a migrare il mio ambiente Elastic Beanstalk Account AWS da uno Account AWS all'altro (Knowledge Center).AWS

Indirizzi IP elastici

È possibile trasferire indirizzi IP elastici tra indirizzi Account AWS che si trovano nello stesso. Regione AWS Per ulteriori informazioni, consulta la sezione Indirizzi IP elastici (documentazione Amazon VPC).

AWS Lambda livelli

Per impostazione predefinita, un AWS Lambda layer creato è privato del tuo Account AWS. Tuttavia, puoi facoltativamente condividere il layer con altri Account AWS o renderlo pubblico. Per copiare

un livello, è necessario riassegnarlo in un altro. Account AWS Per ulteriori informazioni, consulta la sezione Configurazione delle autorizzazioni dei livelli (documentazione Lambda).

Istanze Amazon Lightsail

Puoi creare uno snapshot di un'istanza Amazon Lightsail ed esportare lo snapshot in un'Amazon Machine Image (AMI) e uno snapshot crittografato di un volume Amazon EBS. Per ulteriori informazioni, consulta Esportazione di istantanee EC2 di Amazon Lightsail su Amazon (documentazione Lightsail). Per impostazione predefinita, lo snapshot è crittografato con una chiave gestita AWS creata in AWS Key Management Service (AWS KMS). Tuttavia, questo tipo di chiave KMS non può essere condiviso tra di loro. Account AWS Invece, puoi crittografare manualmente una copia dell'AMI con una chiave gestita dal cliente che può essere utilizzata dall'account di destinazione. Per ulteriori informazioni, consulta Consentire agli utenti di altri account di utilizzare una chiave KMS (AWS KMS documentazione). Puoi quindi condividere l'AMI copiata con la destinazione Account AWS e avviare una nuova EC2 istanza per Lightsail dall'AMI copiata. Per ulteriori informazioni, consulta Avviare un'istanza utilizzando la nuova procedura guidata di avvio dell'istanza (EC2documentazione Amazon).

Cluster Amazon Neptune

Puoi copiare uno snapshot automatico del cluster di database Amazon Neptune su un altro Account AWS. Per ulteriori informazioni, consulta la sezione Copia di uno snapshot del cluster di database (DB) (documentazione Neptune).

Puoi anche condividere uno snapshot manuale con un massimo di 20 Account AWS in grado di ripristinare direttamente un cluster di DB dallo snapshot. Per ulteriori informazioni, consulta la sezione Condivisione di uno snapshot del cluster di database (documentazione Neptune).

Domini Amazon OpenSearch Service

Per copiare dati tra domini Amazon OpenSearch Service, puoi utilizzare Amazon S3 per creare uno snapshot del dominio di origine e quindi ripristinare lo snapshot in un dominio di destinazione in un altro. Account AWS Per ulteriori informazioni, consulta Come posso ripristinare i dati da un dominio Amazon OpenSearch Service in un altro Account AWS (AWS Knowledge Center).

Se disponi di connettività di rete tra i Account AWS, puoi anche utilizzare la funzionalità di replica tra cluster (documentazione OpenSearch del servizio) in OpenSearch Service.

Snapshot di Amazon RDS

Per Amazon Relational Database Service (Amazon RDS) puoi condividere snapshot manuali di istanze o cluster di database con un massimo di 20 Account AWS. Puoi quindi ripristinare l'istanza o il cluster di DB dallo snapshot condiviso. Per ulteriori informazioni, consulta Come posso condividere gli snapshot manuali di Amazon RDS DB o gli snapshot del cluster Aurora DB con un altro Account AWS(Knowledge Center).AWS

Puoi anche usare AWS Database Migration Service (AWS DMS) per configurare la replica continua tra istanze di database in account diversi. Tuttavia, ciò richiede una connettività di rete tra gli account, come il peering VPC o un gateway di transito.

Cluster Amazon Redshift

Per migrare un cluster Amazon Redshift verso un Account AWS altro, devi creare uno snapshot manuale del cluster nell'account di origine, condividere lo snapshot con la Account AWS destinazione e quindi ripristinare il cluster dallo snapshot. Per ulteriori informazioni, consulta Come posso copiare un cluster con provisioning di Amazon Redshift su un altro Account AWS (AWS Knowledge Center).

Domini e zone ospitate di Amazon Route 53

Puoi trasferire domini di Amazon Route 53 tra Account AWS. Per ulteriori informazioni, consulta la sezione Trasferimento di un dominio a un diverso Account AWS (documentazione Route 53).

Puoi anche migrare una zona ospitata da Route 53 a un'altra. Account AWS Per ulteriori informazioni su quando questa procedura è consigliata o richiesta, consulta la sezione Migrazione di una zona ospitata in un altro Account AWS (documentazione Route 53). Quando si esegue la migrazione di una zona ospitata, la si ricrea nell' Account AWS di destinazione. Per istruzioni, consulta la sezione Migrazione di una zona ospitata in un altro Account AWS (documentazione Route 53).

Bucket Amazon S3

Puoi utilizzare la replica nella stessa regione Amazon Simple Storage Service (Amazon S3) per copiare oggetti tra bucket S3 nella stessa regione AWS. Per ulteriori informazioni, consulta la sezione Replica di oggetti (documentazione Amazon S3). Tieni presente quanto segue:

- Cambia la proprietà della replica con Account AWS quella proprietaria del bucket di destinazione. Per istruzioni, consulta la sezione Modifica del proprietario della replica (documentazione Amazon S3).
- Aggiorna le condizioni del proprietario del bucket in modo che riflettano l' Account AWS ID del bucket di destinazione. Per ulteriori informazioni, consulta la sezione Verifica della proprietà del bucket con condizione del proprietario del bucket (documentazione Amazon S3).
- A partire da aprile 2023, l'impostazione forzata del proprietario del bucket è abilitata per i bucket appena creati, rendendo inefficaci gli elenchi di controllo dell'accesso ai bucket () e gli oggetti. ACLs ACLs Per ulteriori informazioni, consulta la pagina dedicata alle modifiche alla sicurezza di Amazon S3 in arrivo (post AWS del blog).
- Puoi usare S3 Batch Replication (documentazione Amazon S3) per replicare oggetti esistenti prima della configurazione della replica.

Modelli Amazon SageMaker AI

SageMaker I modelli di intelligenza artificiale vengono archiviati in un bucket Amazon S3 durante la formazione. Concedendo l'accesso al bucket S3 dall'account di destinazione, puoi implementare un modello memorizzato nell'account di origine sull'account di destinazione. Per ulteriori informazioni, consulta Come posso distribuire un modello Amazon SageMaker AI su un altro Account AWS (AWS Knowledge Center).

AWS WAF web ACLs

AWS WAF le liste di controllo degli accessi Web (web ACLs) devono risiedere nello stesso account delle risorse a cui sono associate, ad esempio CloudFront distribuzioni Amazon, Application Load Balancers, Amazon API Gateway REST e GraphQL. APIs AWS AppSync APIs Puoi utilizzarlo AWS Firewall Manager per gestire centralmente il AWS WAF web ACLs nell'intera organizzazione in e tra le regioni. AWS Organizations Per ulteriori informazioni, consulta la sezione Nozioni di base sulle policy AWS Firewall Manager AWS WAF (documentazione Firewall Manager).

Considerazioni sulla fatturazione durante la transizione a un'architettura multi-account

Se utilizzi AWS Organizations per la transizione a più sistemi Account AWS, puoi utilizzare la funzionalità di fatturazione consolidata (documentazione).AWS Organizations Questa funzione fornisce un'unica fattura combinata che mostra gli addebiti su più account.

Di seguito sono riportate le best practice e i consigli di fatturazione per il passaggio a più account:

- Se hai bisogno di accedere ai tuoi dati di fatturazione storici, prima di accettare l'invito a entrare a far parte di un'organizzazione, crea un report sui costi e sull'utilizzo (AWS Cost and Usage Report documentazione) per esportare i dati di fatturazione storici dell'account in un bucket Amazon Simple Storage Service (Amazon S3). Dopo aver accettato l'invito a entrare a far parte dell'organizzazione, i dati storici di fatturazione dell'account non sono più accessibili.
- Se è necessario unire due organizzazioni, ad esempio per una fusione o un'acquisizione, è possibile utilizzare Account Assessment for AWS Organizations (AWS Solutions Library) per valutare le politiche basate sulle risorse di ciascuna organizzazione e identificare eventuali problemi potenziali prima di combinarli.

Conclusioni

La transizione da un account singolo Account AWS a più account può sembrare inizialmente difficile senza una strategia di adozione. Implementando una strategia multi-account, puoi affrontare molte sfide che le aziende devono affrontare quando utilizzano un singolo Account AWS:

- Confondere i dati di produzione con i dati di sviluppo: è possibile concedere autorizzazioni e accessi diversi utilizzando, AWS IAM Identity Center con set di autorizzazioni separati, unità organizzative di produzione e non di produzione. Solo gli utenti con privilegi elevati dovrebbero avere accesso al database di produzione e tale accesso dovrebbe avvenire per periodi di tempo limitati ed essere controllato.
- Implementazione della produzione che influisce su altre operazioni aziendali: puoi separare le parti interessate utilizzando più account e più ambienti. Ad esempio, puoi creare un ambiente dimostrativo di vendita dedicato, all'interno di un account non di produzione, in modo da poter pianificare le implementazioni e i rilasci quando non sono previste dimostrazioni.
- Rallentamento delle prestazioni del carico di lavoro di produzione durante il test dei carichi di lavoro di sviluppo: ciascuna di esse prevede quote di servizio indipendenti Account AWS che regolano ogni servizio. Utilizzando più account, puoi limitare l'ambito di un ambiente che influisce su un altro ambiente.
- Distinzione dei costi di produzione dai costi di sviluppo: la fatturazione consolidata per l'organizzazione riassume tutti i costi a livello di Account AWS in modo che il team finanziario possa vedere i costi di produzione rispetto agli ambienti non di produzione, come gli ambienti di sviluppo, test e demo. Puoi anche utilizzare tag e policy di assegnazione dei tag per separare i costi all'interno di un account.
- Limitazione dell'accesso ai dati sensibili: IAM Identity Center consente di disporre di policy di accesso separate per un gruppo di persone associate a un account specifico.
- Controllo dei costi: utilizzando le politiche di controllo dei servizi (SCPs) in un'architettura multi-account, è possibile impedire l'accesso a servizi specifici Servizi AWS che potrebbero comportare costi elevati per l'organizzazione. SCPs può negare qualsiasi accesso a servizi specifici o limitare l'utilizzo di un servizio a un tipo specifico, ad esempio limitando i tipi di istanze Amazon Elastic Compute Cloud (Amazon EC2) che possono essere create.

Collaboratori

Hanno collaborato alla stesura del presente documento:

- Justin Plock, Principal Solutions Architect, AWS (autore principale)
- Emily Arnautovic, architetto principale, AWS
- Jason, architetto senior delle DiDomenico soluzioni, AWS
- Michael Leighty, architetto senior specializzato in soluzioni di sicurezza, AWS
- Jesse Lepich, architetto senior specializzato in soluzioni di sicurezza, AWS
- Rodney Lester, architetto principale delle soluzioni, AWS
- Israele Lopez Moriano, architetto delle soluzioni, AWS
- George Rolston, architetto senior delle soluzioni, AWS
- Alex Torres, architetto senior delle soluzioni, AWS
- Dave Walker, architetto principale delle soluzioni, AWS

Risorse

AWS Guida prescrittiva

- AWS Startup Security Baseline (SSB)AWS
- AWS Architettura di riferimento per la sicurezza (AWS SRA)
- Le 10 migliori pratiche di sicurezza per proteggere i backup in AWS

AWS post sul blog

- In che modo la configurazione degli utenti e dei ruoli IAM può aiutarti a proteggere la tua startup
- Come consentire agli sviluppatori di creare risorse IAM migliorando al contempo la sicurezza e l'agilità dell'organizzazione

AWS white paper

- Organizzazione dell' AWS ambiente utilizzando più account
- Stabilisci la tua Cloud Foundation su AWS
- Creazione di un'infrastruttura di rete AWS multi-VPC scalabile e sicura

AWS esempi di codice

- Automatizza la configurazione dei servizi di sicurezza con AWS Control Tower () GitHub

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
Politiche di controllo delle risorse	Abbiamo aggiunto informazioni sulle politiche di controllo delle risorse nella sezione Configurare un'organizzazione.	20 novembre 2024
Best practice centralizzate in materia di uscita	Abbiamo aggiornato le migliori pratiche per proteggere il traffico in uscita.	6 maggio 2024
Best Practice dell'organizzazione	Abbiamo aggiornato le best practice per la creazione di un'organizzazione in AWS Organizations.	4 dicembre 2023
Considerazioni sulla fatturazione	Abbiamo aggiunto la sezione Considerazioni sulla fatturazione.	20 settembre 2023
Migrazione delle risorse, connettività delle applicazioni e Amazon VPC Lattice	Abbiamo aggiunto le sezioni Migrazione delle risorse e Connessione delle applicazioni. Abbiamo anche aggiunto informazioni su un nuovo Servizio AWS, Amazon Virtual Private Cloud (Amazon VPC) Lattice.	27 aprile 2023
Cronologia dell'account e ABAC	Abbiamo modificato la sezione Crea una landing zone per aggiungere informazioni su come fare in modo che i tuoi	6 gennaio 2023

	nuovi dispositivi Account AWS abbiano una cronologia di utilizzo in modo che tu possa aggiungerli alla tua AWS Control Tower landing zone. Abbiamo anche rivisto la sezione Aggiunta di utenti iniziali per aggiungere informazioni su come utilizzare il controllo degli accessi basato su attributi (ABAC) per far passare il metodo di autenticazione da un IdP esterno basato su SAML a AWS IAM Identity Center.	
Rete del traffico in uscita	Abbiamo rivisto la sezione di uscita centralizzata per aggiungere informazioni sull'utilizzo del firewall Amazon Route 53 Resolver DNS per limitare il traffico in uscita a nomi di dominio specifici.	13 ottobre 2022
Sicurezza del traffico in uscita	Abbiamo aggiunto la sezione Best practice per proteggere il traffico in uscita.	6 ottobre 2022
Limiti delle autorizzazioni	Abbiamo migliorato la definizione di un limite delle autorizzazioni, e nella sezione Risorse, abbiamo aggiunto un nuovo link per ulteriori informazioni su questo argomento.	22 settembre 2022
Pubblicazione iniziale	—	6 settembre 2022

AWS Glossario delle linee guida prescrittive

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

Numeri

7 R

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

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

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

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

migrazione attiva-passiva

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

funzione aggregata

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

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

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

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

AWS Workload Qualification Framework (WQF)AWS

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

B

bot difettoso

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

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

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

Classificazione binaria

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

filtro Bloom

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

distribuzioni blu/verdi

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

bot

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

botnet

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

ramo

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

accesso break-glass

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

strategia brownfield

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

cache del buffer

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

capacità di business

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

pianificazione della continuità operativa (BCP)

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

C

CAF

Vedi AWS Cloud Adoption Framework.

implementazione canaria

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

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

Centro di eccellenza cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

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

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

CMDB

Vedi database di gestione della configurazione.

repository di codice

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

cache fredda

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

dati freddi

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

visione artificiale (CV)

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

deriva della configurazione

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

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

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

CV

Vedi visione artificiale.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

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

deriva dei dati

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

dati in transito

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

rete di dati

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di definizione del database.

deep ensemble

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

deep learning

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

defense-in-depth

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

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

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

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

gemello digitale

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

tabella delle dimensioni

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

disastro

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

disaster recovery (DR)

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

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

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

DOTT.

Vedi disaster recovery.

rilevamento della deriva

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

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

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

scambio elettronico di dati (EDI)

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

crittografia

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

chiave crittografica

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

endianità

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

endpoint

Vedi service endpoint.

servizio endpoint

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

pianificazione delle risorse aziendali (ERP)

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

crittografia envelope

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

ambiente

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

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

epica

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

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

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

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

F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

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

prompt con pochi scatti

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

Vedi il modello di base.

modello di fondazione (FM)

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

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

G

AI generativa

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

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

immagine dorata

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

strategia greenfield

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

guardrail

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

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

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

alta disponibilità (HA)

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

modernizzazione storica

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

dati di esclusione

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

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

I

IaC

Considera l'infrastruttura come codice.

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

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

VPC in ingresso (ingress)

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

migrazione incrementale

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

IIoInternet delle cose industriale (T)

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

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

modello linguistico di grandi dimensioni (LLM)

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

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

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

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

ramo principale

Vedi filiale.

malware

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

servizi gestiti

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

sistema di esecuzione della produzione (MES)

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

MAP

Vedi Migration Acceleration Program.

meccanismo

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

account membro

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

MEH.

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

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

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

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

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

migrazione su larga scala

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

fabbrica di migrazione

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

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

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

Vedi machine learning.

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

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

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

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

infrastruttura mutabile

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

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

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

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

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

OPC-UA

Vedi Open Process Communications - Unified Architecture.

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

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

tecnologia operativa (OT)

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

integrazione delle operazioni (OI)

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

trail organizzativo

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

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

gestione del cambiamento organizzativo (OCM)

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

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

ORR

Vedi la revisione della prontezza operativa.

- NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

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

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

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

persistenza poliglotta

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

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

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

concatenamento rapido

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

pseudonimizzazione

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

publish/subscribe (pub/sub)

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

Q

Piano di query

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

regressione del piano di query

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

R

Matrice RACI

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

STRACCIO

Vedi Retrieval Augmented Generation.

ransomware

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

Matrice RASCI

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

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

Regione

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

regressione

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

riospitare

Vedi 7 R.

rilascio

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

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

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

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi l'obiettivo del punto di ripristino.

RTO

Vedi l'obiettivo del tempo di ripristino.

runbook

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

S

SAML 2.0

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

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

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

sicurezza fin dalla progettazione

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

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

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

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

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

Modello di responsabilità condivisa

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

SIEM

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

punto di errore singolo (SPOF)

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

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

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

SPOF

Vedi punto di errore singolo.

schema a stella

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

modello del fico strangolatore

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

sottorete

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

controllo di supervisione e acquisizione dati (SCADA)

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

crittografia simmetrica

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

test sintetici

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

prompt di sistema

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

T

tags

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

variabile di destinazione

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

elenco di attività

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

Ambiente di test

Vedi ambiente.

training

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

Transit Gateway

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

flusso di lavoro basato su trunk

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

Accesso attendibile

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

regolazione

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

team da due pizze

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

U

incertezza

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

compiti indifferenziati

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

ambienti superiori

Vedi ambiente.

V

vacuum

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

controllo delle versioni

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

Peering VPC

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

vulnerabilità

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

W

cache calda

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

dati caldi

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

funzione finestra

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

Carico di lavoro

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

flusso di lavoro

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

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

Z

exploit zero-day

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

vulnerabilità zero-day

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

prompt zero-shot

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

applicazione zombie

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

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