Guida alla sicurezza e al funzionamento dell'Autonomous Driving Data Framework (ADDF)

AWS Linee guida prescrittive

AWS Linee guida prescrittive: Guida alla sicurezza e al funzionamento dell'Autonomous Driving Data Framework (ADDF)

Table of Contents

Guida alla sicurezza e al funzionamento dell'Autonomous Driving Data Framework (ADDF)

Andreas Falkenberg, Junjie Tang, Torsten Reitemeyer e Srinivas Reddy Cheruku, Amazon Web Services

Novembre 2022 (cronologia dei documenti)

L'Autonomous Driving Data Framework (ADDF) è un progetto open-source ideato per fornire artefatti di codice riutilizzabili e modulari ai team del settore automobilistico che desiderano implementare attività comuni per i sistemi avanzati di assistenza alla guida (ADAS), come la configurazione dell'archiviazione di dati centralizzata, delle pipeline di elaborazione dei dati, dei meccanismi di visualizzazione, delle interfacce di ricerca, dei carichi di lavoro di simulazione, delle interfacce di analisi e dei pannelli di controllo preconfigurati. Utilizzando l'ADDF è possibile condividere, modificare o creare moduli completamente personalizzabili che riducono lo sforzo richiesto per creare e implementare queste soluzioni.

Questa guida ha lo scopo di aiutare a comprendere le best practice per implementare e utilizzare in modo sicuro l'ADDF nel Cloud AWS, e tratta i seguenti argomenti:

- Architettura e terminologia: esamina l'architettura generale, i flussi di lavoro e i termini importanti.
- Modello di responsabilità condivisa— Comprendi il tuo ruolo e il ruolo che svolgi nella protezione AWS della distribuzione di ADDF e delle risorse cloud.
- Processo di revisione della sicurezza— Poiché ADDF è un progetto open source, scopri come AWS e i collaboratori completano le revisioni di sicurezza.
- Funzionalità di sicurezza integrate: scopri come le best practice e le funzionalità di sicurezza sono integrate nel progetto open source ADDF e nel suo framework di implementazione.
- Configurazione e funzionamento sicuri: scopri come implementare e utilizzare l'ADDF nel Cloud AWS.

Destinatari principali

Questa guida è destinata ai team delle operazioni di sviluppo (DevOps), agli ingegneri dell'infrastruttura, agli amministratori, al personale della sicurezza IT e ai team di risposta agli incidenti che hanno il compito di valutare, implementare, personalizzare e utilizzare ADDF. È

possibile applicare i consigli contenuti in questa guida per i nostri ambienti di produzione. proof-of-concept

Questa guida presuppone che l'utente non abbia alcuna conoscenza precedente dell'ADDF. Tuttavia, si consiglia di leggere il file readme (GitHub) di ADDF prima di procedere.

Obiettivi aziendali specifici

Questa guida è progettata per aiutarti a configurare e utilizzare l'ADDF in modo più sicuro e protetto negli ambienti di sviluppo e produzione.

Terminologia e architettura dell'ADDF

Per poter comprendere gli argomenti operativi e di sicurezza di questa guida, è necessaria una conoscenza approfondita della terminologia, dei componenti e dell'architettura dell'Autonomous Driving Data Framework (ADDF). Questa sezione contiene i seguenti argomenti:

Terminologia dell'ADDF

La terminologia chiave dell'ADDF è la seguente:

- Modulo ADDF: un modulo è un'infrastruttura come codice (IaC) che implementa un'attività comune in un sistema avanzato di assistenza alla guida (advanced driver-assistance system, ADAS). Le attività più comuni includono la configurazione dell'archiviazione di dati centralizzata, le pipeline di elaborazione dati, i meccanismi di visualizzazione, le interfacce di ricerca, i carichi di lavoro di simulazione, le interfacce di analisi e i pannelli di controllo predefiniti. È possibile creare un modulo in base alle proprie esigenze oppure riutilizzare o personalizzare un modulo esistente.

  È possibile utilizzare AWS Cloud Development Kit (AWS CDK) per definire i moduli ADDF oppure è possibile utilizzare qualsiasi framework IaC comune, come Hashicorp Terraform o AWS CloudFormation, per implementare i moduli ADDF. I moduli hanno una serie di parametri di input. I parametri di input possono dipendere dai valori di output di altri moduli. Il modulo ADDF è l'unità di implementazione più piccola per un Account AWS di destinazione dell'ADDF.
- File manifesto dell'implementazione dell'ADDF: questo file definisce un'orchestrazione di moduli ADDF autonomi. L'orchestrazione si riferisce all'ordine di implementazione dei moduli. Nel file manifesto dell'implementazione dell'ADDF, è possibile utilizzare gruppi ADDF per raggruppare i moduli correlati. In questo file, si definiscono anche la toolchain Account AWS ADDF, la destinazione ADDF e la destinazione. Account AWS Regioni AWS
- Framework di distribuzione ADDF: questo framework distribuisce i moduli ADDF nella destinazione ADDF in Account AWS base all'orchestrazione definita nel file manifesto di distribuzione ADDF. Il framework di distribuzione ADDF viene implementato utilizzando i seguenti progetti open source: AWS

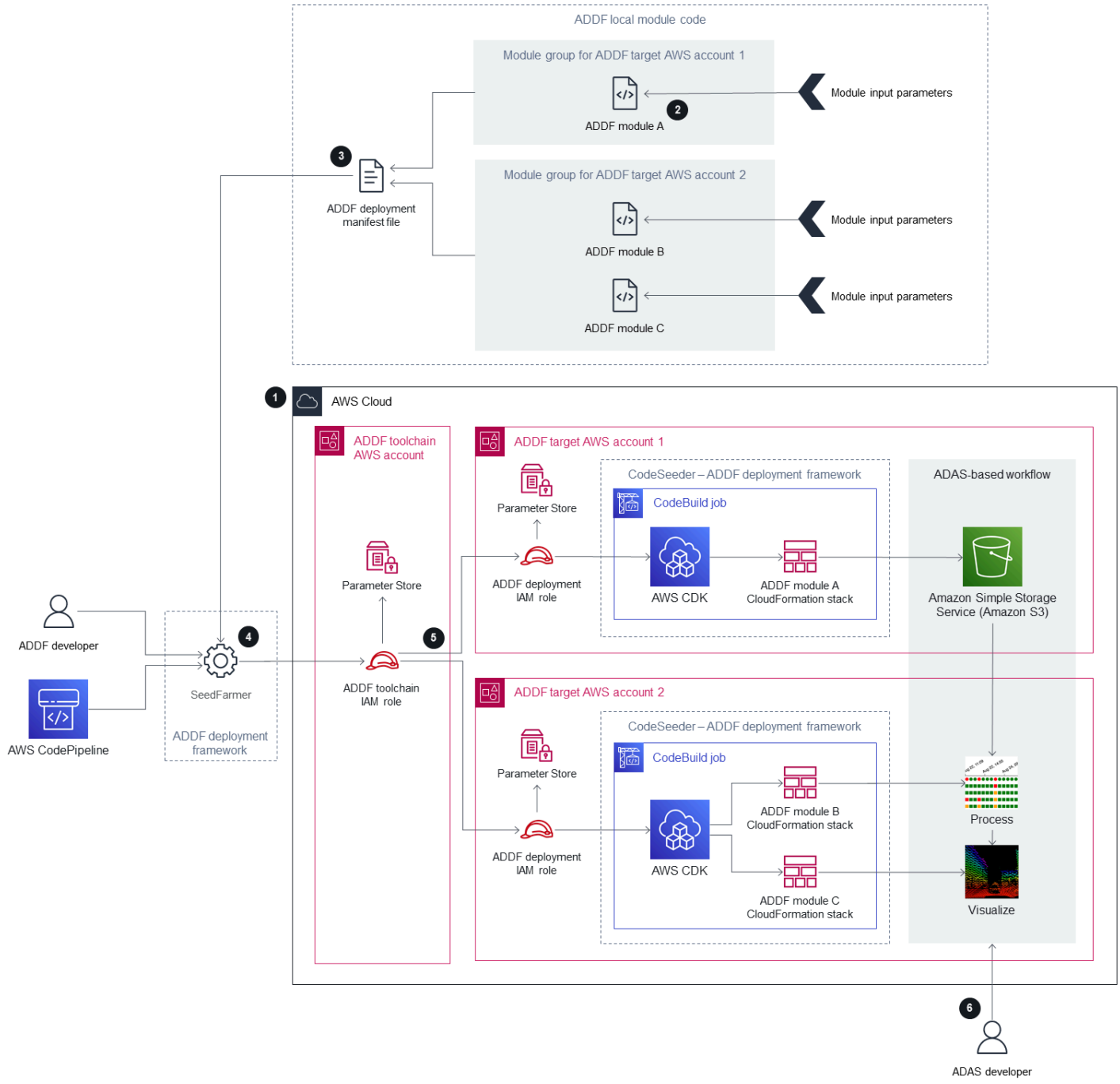
- SeedFarmer(GitHub) — SeedFarmer è lo strumento CLI utilizzato per le distribuzioni ADDF. Gestisce ogni stato del modulo, prepara e impacchetta il codice del modulo, crea le politiche con privilegi minimi per i ruoli di distribuzione ADDF e fornisce istruzioni semantiche da utilizzare per la distribuzione. CodeSeeder È possibile interagire direttamente con le distribuzioni ADDF SeedFarmer per eseguire o integrarle in una pipeline di integrazione e distribuzione continua (CI/CD).
- CodeSeeder(GitHub) — CodeSeeder distribuisce un'infrastruttura arbitraria come pacchetti di codice tramite un processo. AWS CodeBuild SeedFarmerorchestra ed esegue automaticamente. CodeSeeder Interagisce SeedFarmer direttamente solo con. CodeSeeder

Il framework di implementazione ADDF è progettato per supportare le implementazioni in architetture ad account singolo e multi-account. In base ai requisiti dell'organizzazione, si può decidere se è necessaria un'architettura ad account singolo o multi-account.

- Toolchain ADDF Account AWS: questo account orchestra e gestisce la distribuzione dei moduli nella destinazione ADDF Account AWS, in base alle definizioni nel file manifesto di distribuzione ADDF. Un'implementazione dell'ADDF può avere un solo Account AWS toolchain ADDF. In un'architettura ad account singolo, l' Account AWS toolchain ADDF è anche l' Account AWS di destinazione dell'ADDF. Questo account contiene un ruolo AWS Identity and Access Management (IAM), chiamato ruolo IAM della toolchain ADDF, che viene assunto da durante il processo di distribuzione ADDF. SeedFarmer In questa guida, facciamo riferimento a una toolchain ADDF come a un account toolchain Account AWS .
- Target ADDF Account AWS: questi sono gli account di destinazione in cui vengono distribuiti i moduli ADDF. È possibile avere uno o più account di destinazione. Questi account contengono le risorse e la logica dell'applicazione descritte nel file manifesto dell'implementazione dell'ADDF e nei relativi moduli mappati. In un'architettura a account singolo, il target ADDF Account AWS è anche la toolchain ADDF. Account AWS Ogni account di destinazione ADDF contiene un ruolo IAM, chiamato ruolo IAM di implementazione ADDF, che viene assunto da durante il processo di distribuzione. CodeSeeder In questa guida, facciamo riferimento a un target ADDF Account AWS come a un account di destinazione.
- Istanza ADDF: quando si implementano l'ADDF e i propri moduli nel cloud, come definito nel file manifesto dell'implementazione dell'ADDF, diventano un'istanza ADDF. Un'istanza ADDF può avere un'architettura ad account singolo o multi-account ed è possibile implementare più istanze ADDF. Per ulteriori informazioni sulla scelta del numero di istanze e sulla progettazione dell'architettura dell'account per il tuo caso d'uso, vedi Definizione dell'architettura dell'ADDF.

Architettura dell'ADDF

Il diagramma seguente mostra un'architettura di alto livello per un'istanza ADDF nel Cloud AWS. Mostra un'architettura multi-account che include un account toolchain dedicato e due account di destinazione. Questa guida illustra il end-to-end processo di utilizzo di ADDF per distribuire risorse agli account di destinazione.



1. Creazione e bootstrap dell' Account AWS ADDF.

   Per funzionare correttamente, ogni account deve essere sottoposto a bootstrap sull'ADDF e su AWS CDK. Se si tratta di una nuova implementazione dell'ADDF o stai aggiungendo nuovi account di destinazione, procedi come segue:

   a. Bootstrap AWS CDK nell'account della toolchain e in ogni account di destinazione. Per istruzioni, consulta Bootstrapping (documentazione AWS CDK). ADDF utilizza AWS CDK per implementare la propria infrastruttura.

   b. Bootstrap dell'ADDF nell'account toolchain e in ogni account di destinazione. Per istruzioni, consulta Bootstrap Account AWS(s) nella ADDF Deployment Guide. Questo imposta tutti i ruoli IAM specifici di ADDF richiesti da e. SeedFarmer CodeSeeder

   > **Note**
   >
   > Devi eseguire questo passaggio solo se stai eseguendo l'implementazione iniziale dell'ADDF o se stai aggiungendo nuovi account di destinazione. Questo passaggio non fa parte delle implementazioni ADDF ricorrenti su istanze ADDF già stabilite.

2. Crea o personalizza i moduli ADDF.

   Crea o personalizza i moduli ADDF in base al problema specifico da risolvere. Il modulo dovrebbe rappresentare un'attività isolata o un gruppo di attività isolato. Definisci i parametri di input per il modulo secondo necessità e usa i valori di output del modulo come parametri di input per altri moduli.

3. Definisci l'orchestrazione del modulo nel file manifesto dell'implementazione dell'ADDF.

   Nel file manifesto dell'ADDF, organizza i moduli in gruppi e definisci l'ordine di implementazione e le dipendenze tra di essi. In questo file, specificate anche il singolo account della toolchain e gli account di destinazione (inclusi Regioni AWS) per ogni gruppo ADDF e i relativi moduli.

4. Valuta il file manifesto dell'implementazione dell'ADDF e stabilisci l'ambito di implementazione.

   Lo sviluppatore ADDF o una pipeline CI/CD, ad esempio AWS CodePipeline, avvia una valutazione del file manifesto di distribuzione ADDF chiamando lo strumento CLI,. SeedFarmer Per iniziare la valutazione:

   - SeedFarmer utilizza il file manifesto di distribuzione ADDF come parametro di input per la valutazione.

- Per assumere il ruolo IAM della toolchain ADDF, SeedFarmer si prevede lo stesso ruolo IAM o le stesse credenziali utente valide definite durante il processo di bootstrap ADDF, nel passaggio 1.

Se SeedFarmer non dispone delle credenziali corrette per assumere il ruolo IAM della toolchain ADDF o non può accedere al file manifesto di distribuzione ADDF, la valutazione non viene avviata.

Se SeedFarmer può avviare la valutazione, assume il ruolo IAM della toolchain ADDF nell'account della toolchain. Da lì, SeedFarmer può accedere a qualsiasi account di destinazione, assumendo il ruolo IAM di implementazione ADDF in quell'account. SeedFarmer quindi prova a leggere tutti i metadati ADDF nell'account della toolchain e negli account di destinazione. Si verifica una delle seguenti situazioni:

- Se non ci sono metadati ADDF da leggere, ciò indica che si tratta di una nuova istanza ADDF. SeedFarmer determina che l'ambito di distribuzione è l'intero file manifesto di distribuzione ADDF e il relativo contenuto.
- Se esistono metadati ADDF, SeedFarmer confronta il file manifesto di distribuzione ADDF e il relativo contenuto con gli MD5 hash degli artefatti distribuiti esistenti negli account di destinazione. Se vengono rilevate modifiche che possono essere implementate, questo processo continua. Se non viene rilevata alcuna modifica da implementare, il processo è completato.

5. Implementa i moduli ADDF pertinenti negli account di destinazione.

   CodeSeeder ora dispone di un elenco ordinato di distribuzioni da eseguire, in base al file manifesto di distribuzione ADDF e ai risultati della valutazione del passaggio precedente. In base a tale elenco ordinato, CodeSeeder presuppone il ruolo IAM di implementazione ADDF in ogni account di destinazione associato. Viene quindi eseguito CodeSeeder in un AWS CodeBuild processo per creare o aggiornare le singole distribuzioni IaC, ad esempio le AWS CDK applicazioni, per il modulo ADDF. Per impostazione predefinita, ADDF utilizza AWS CDK come framework IAc, ma sono supportati anche altri framework IAc comuni. Una volta completato il processo per ogni account di destinazione, si dispone di un flusso di lavoro completamente distribuito, su più account e end-to-end basato su ADAS, come definito nel file manifesto di distribuzione ADDF.

   Se usi un'architettura ad account singolo, l'account toolchain e gli account di destinazione sono lo stesso account, e questo account unico dispone di tutte le funzionalità descritte in precedenza.

6. Usa l'infrastruttura implementata dall'ADDF.

Uno sviluppatore ADAS può utilizzare il flusso di lavoro basato sull'ADAS distribuito in base al caso d'uso.

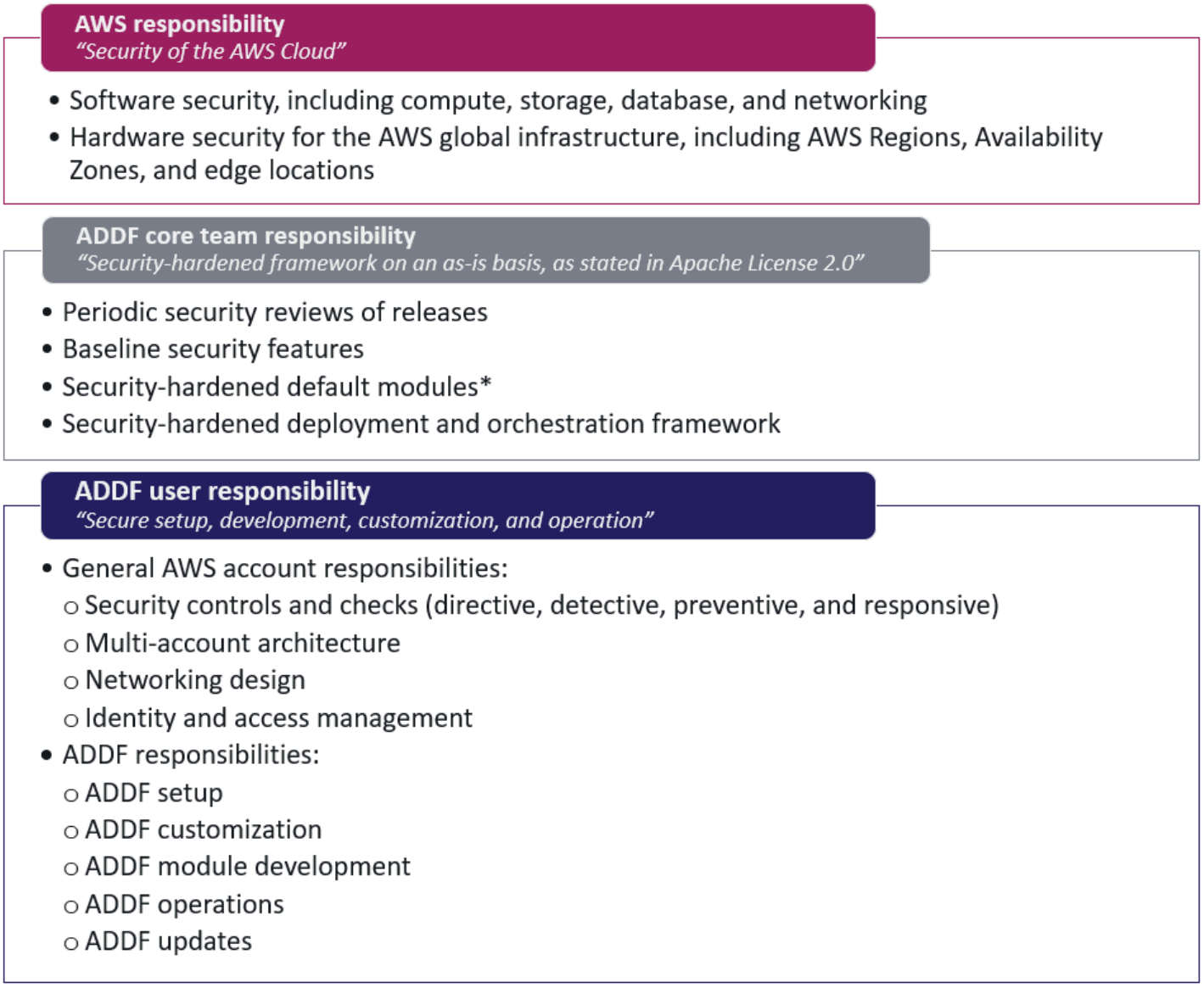
Questo flusso di lavoro descrive l'architettura di una singola istanza di un ambiente multi-account ADDF. A seconda del modello di sviluppo, implementazione e funzionamento, si consiglia di eseguire più istanze ADDF in un ambiente a più fasi. Una configurazione tipica potrebbe includere un'istanza ADDF dedicata dedicata a ciascuna fase di distribuzione, ad esempio filiali Account AWS per lo sviluppo, il test e la produzione. È inoltre possibile eseguire più istanze ADDF nello stesso ambiente con account singolo o multiaccount nello stesso ambiente Regione AWS, supponendo di aver creato uno spazio dei nomi di risorse univoco per ogni istanza ADDF. Per ulteriori informazioni, consulta Definizione dell'architettura dell'ADDF.

Modello di responsabilità condivisa per l'ADDF

Il modello di responsabilità condivisa che si applica a si applica Servizi AWS anche all'Autonomous Driving Data Framework (ADDF). Le seguenti entità hanno la responsabilità condivisa di proteggere l'ADDF come indicato nel diagramma seguente:

- AWS— L'offerta Servizi AWS del fornitore di infrastrutture cloud.
- Team principale ADDF: il team principale di ADDF è l'entità che pubblica le versioni ADDF nel repository ADDF (). GitHub
- Utente dell'ADDF: gli utenti dell'ADDF includono, a titolo esemplificativo,
  - Sviluppatore ADDF: chiunque modifichi, personalizzi o crei nuovo codice del modulo ADDF.
  - Operatore ADDF: chiunque configuri e gestisca un'istanza ADDF.
  - Sviluppatore ADAS: l'utente finale o il consumatore delle risorse distribuite dall'ADDF. Ad esempio, uno sviluppatore ADAS può interrogare un frontend di visualizzazione creato come parte dell'implementazione dell'ADDF.

Il diagramma seguente riassume la responsabilità condivisa tra AWS il core team ADDF e l'utente ADDF.



* Excluding any modules in the ADDF **/modules/demo-only/** folder. Those modules exist only for proof-of-concept purposes and didn't receive security hardening.

AWS responsabilità

AWS è responsabile della protezione dell'infrastruttura che gestisce tutti i servizi offerti nel Cloud AWS, come definito nel modello di responsabilitàAWS condivisa. Questa infrastruttura è composta da hardware, software, rete e strutture che eseguono Cloud AWS i servizi.

Responsabilità del core team ADDF

Il team principale di ADDF fornisce un framework di per sé sicuro, con il massimo impegno possibile, in base alla licenza Apache 2.0 (). GitHub Il core team ADDF è responsabile di quanto segue:

- Revisioni periodiche della sicurezza delle versioni
- Funzionalità di sicurezza di base
- Moduli predefiniti con protezione avanzata (ciò esclude tutti i moduli nella cartella. `/modules/demo-only/` Questi moduli sono utilizzati solo per proof-of-concept scopi specifici e non sono sottoposti a misure di protezione avanzate.)
- Framework di implementazione e orchestrazione rafforzato dal punto di vista della sicurezza

Queste responsabilità in materia di sicurezza si estendono solo al framework, così come fornito nel GitHub repository, senza alcuna modifica o personalizzazione. Ciò include tutti i moduli ADDF, ad eccezione dei moduli ADDF presenti nella cartella `modules/demo-only/`. I moduli ADDF in questa cartella non sono protetti e non devono essere implementati in ambienti di produzione o in qualsiasi ambiente con dati sensibili o protetti. Questi moduli sono inclusi per mostrare le funzionalità del sistema e possono essere utilizzati come base per creare moduli personalizzati e dotati di protezione avanzata.

> **Note**
>
> L'ADDF come framework viene fornito così com'è. Non comporta alcuna responsabilità e garanzia, come indicato nella licenza Apache 2.0 (). GitHub È necessario effettuare una valutazione della sicurezza dell'ADDF e verificare che sia conforme ai requisiti di sicurezza specifici della propria organizzazione.

Responsabilità dell'utente dell'ADDF

L'ADDF e i suoi moduli sono sicuri solo se l'ADDF è configurato, personalizzato e gestito in modo sicuro. L'utente dell'ADDF è pienamente responsabile della sicurezza di quanto segue:

- Account AWS Responsabilità generali:
  - Controlli di sicurezza (direttivi, di rilevamento, preventivi e reattivi)
  - Architettura multi-account

  - Progettazione della rete
  - Gestione dell’identità e degli accessi
- Responsabilità specifiche per l'ADDF:
  - Configurazione dell'ADDF
  - Personalizzazione dell'ADDF
  - Sviluppo del modulo ADDF
  - Operazioni ADDF
  - Aggiornamenti dell'ADDF

Account AWS Responsabilità generali

Prima di distribuire qualsiasi risorsa relativa ad ADDF Account AWS, è Account AWS necessario configurarla secondo le migliori pratiche del Well-Architected AWS Framework. Ciò include controlli di sicurezza direttivi, di rilevamento, preventivi e reattivi. È necessario disporre di processi di mitigazione dettagliati, in caso di violazioni o incidenti di sicurezza. La policy dell'organizzazione dovrebbe includere requisiti per la gestione centralizzata dell'identità, dell'accesso e delle reti. Di solito, questi requisiti e servizi sono gestiti da un team dedicato alla zona di destinazione.

Responsabilità specifiche per l'ADDF

Configurazione sicura dell'ADDF

La responsabilità di un utente dell'ADDF parte dalla configurazione sicura dell'ADDF secondo la documentazione ADDF. Ti consigliamo vivamente di seguire le istruzioni contenute nella ADDF Deployment Guide (). GitHub Per ulteriori informazioni sulla configurazione sicura dell'ADDF, consulta Definizione dell'architettura dell'ADDF e Configurazione iniziale dell’.

Personalizzazione sicura dell'ADDF

In caso di personalizzazione delle funzionalità principali di ADDF, come i moduli principali ADDF CodeSeeder SeedFarmer, l'utente ADDF si assume la piena responsabilità di tali modifiche. Per ulteriori informazioni, consulta Personalizzazione del codice del framework di implementazione ADDF.

Sviluppo sicuro del modulo ADDF

L'utente dell'ADDF è pienamente responsabile di qualsiasi modulo personalizzato implementato utilizzando l'ADDF. Inoltre, l'utente dell'ADDF è responsabile di eventuali modifiche al codice dei moduli forniti dall'ADDF. Per ulteriori informazioni, consulta Scrivere moduli personalizzati nell'ADDF.

Aggiornamenti e operazioni ADDF sicuri

Man mano che si evolve, l'ADDF riceve aggiornamenti di funzionalità e sicurezza. È responsabilità dell'utente ADDF controllare regolarmente gli aggiornamenti pubblicati nell' GitHub archivio e utilizzare ADDF in modo sicuro a lungo termine. Per ulteriori informazioni, consulta Implementazioni ADDF ricorrenti, Controlli di sicurezza ricorrenti, Aggiornamenti dell'ADDF e Disattivazione.

Processo di revisione della sicurezza dell'ADDF

L'Autonomous Driving Data Framework (ADDF) è stato creato pensando alla sicurezza. Prima del rilascio al pubblico, AWS ha eseguito una revisione interna iniziale della sicurezza dell'ADDF e ha risolto i problemi di sicurezza identificati. Entrambi AWS e la comunità open source contribuiscono alle continue revisioni della sicurezza del framework.

Revisioni periodiche della sicurezza effettuate da AWS

ADDF è pubblicato sotto l' GitHub organizzazione awslabs di proprietà di. AWS AWS esegue regolarmente revisioni di sicurezza automatiche e manuali del codice in questa organizzazione, per verificare la sicurezza con la massima diligenza. In base alla AWS politica, AWS non divulga informazioni sulla frequenza delle revisioni di sicurezza, sull'approccio o sugli strumenti utilizzati. Inoltre, AWS non pubblica alcun rapporto di audit interno su ADDF. Tuttavia, tutti i problemi di sicurezza identificati vengono corretti e pubblicati tramite richiesta pull con urgenza elevata.

> **Note**
>
> Il framework ADDF viene fornito «COSÌ COM'È», SENZA GARANZIE O CONDIZIONI DI ALCUN TIPO, esplicite o implicite, incluse, a titolo esemplificativo, qualsiasi garanzia o condizione di titolo, non violazione, commerciabilità o idoneità per uno scopo particolare, come indicato nella licenza Apache 2.0 (). GitHub L'utente è tenuto a condurre la propria valutazione della sicurezza dell'ADDF e verificare se sia conforme ai requisiti di sicurezza specifici della propria organizzazione e, come stabilito nella licenza Apache 2.0, l'utente è l'unico responsabile della determinazione dell'adeguatezza all'uso della ridistribuzione dell'ADDF e si assume tutti i rischi associati all'esercizio o ai permessi concessi da tale licenza.

Revisioni e contributi open source sulla sicurezza

ADDF è un progetto open source che accoglie contributi. Invitiamo tutti gli utenti a effettuare la propria revisione della sicurezza del framework e a contribuire segnalando eventuali esiti relativi alla sicurezza. Se trovi un problema nel codice, segui le linee guida riportate in Notifiche relative ai problemi di sicurezza (documentazione ADDF).

Funzionalità di sicurezza integrate nell'ADDF

L'Autonomous Driving Data Framework (ADDF) dispone di diverse funzionalità di sicurezza integrate. Per impostazione predefinita, queste funzionalità sono progettate per aiutarti a configurare un framework sicuro e consentire alla tua organizzazione di soddisfare i requisiti di sicurezza aziendali comuni.

Le funzionalità di sicurezza integrate sono le seguenti:

- Privilegio minimo per il codice del modulo ADDF
- Infrastruttura come codice
- Controlli di sicurezza automatizzati per l'IaC
- Politica personalizzata di minimo privilegio per il ruolo di distribuzione AWS CDK
- Policy del privilegio minimo per il file deployspec del modulo
- Crittografia dei dati
- Archiviazione delle credenziali tramite Secrets Manager
- Recensioni di sicurezza di e SeedFarmer CodeSeeder
- Autorizzazioni, limiti, supporto per il ruolo di AWS CodeBuild CodeSeeder
- AWS architettura multi-account
- Autorizzazioni con privilegi minimi per e implementazioni multi-account

Privilegio minimo per il codice del modulo ADDF

Il privilegio minimo è 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. I moduli forniti dall'ADDF seguono rigorosamente il principio del privilegio minimo nel codice e nelle risorse implementate, rispettando i seguenti punti:

- Tutte le policy AWS Identity and Access Management (IAM) generate per un modulo ADDF dispongono delle autorizzazioni minime necessarie per il caso d'uso.
- Servizi AWS sono configurati e implementati secondo il principio del privilegio minimo. I moduli forniti dall'ADDF usano solo i servizi e le funzionalità del servizio necessari per il caso d'uso specifico.

Infrastruttura come codice

L'ADDF, come framework, è progettato per implementare i moduli ADDF come infrastruttura come codice (IaC). L'IaC elimina i processi di implementazione manuali e aiuta a prevenire gli errori e le configurazioni sbagliate che possono derivare dai processi manuali.

L'ADDF è progettato per orchestrare e implementare moduli utilizzando tutti i framework IaC comuni. Questi includono, a titolo esemplificativo ma non esaustivo:

- AWS Cloud Development Kit (AWS CDK)
- AWS CloudFormation
- Hashicorp Terraform

È possibile utilizzare diversi framework IaC per scrivere moduli diversi e poi usare l'ADDF per implementarli.

Il framework IaC predefinito utilizzato dai moduli ADDF è. AWS CDK AWS CDK è un'astrazione orientata agli oggetti di alto livello che è possibile utilizzare per definire le risorse in modo imperativo. AWS AWS CDK applica già di default le migliori pratiche di sicurezza per vari servizi e scenari. Grazie all'utilizzo AWS CDK, si riduce il rischio di configurazioni errate della sicurezza.

Controlli di sicurezza automatizzati per l'IaC

L'utilità cdk-nag open source () GitHub è integrata in ADDF. Questa utilità verifica automaticamente la conformità dei moduli ADDF basati su alle migliori pratiche AWS CDK generali e di sicurezza. L'utility cdk-nag usa regole e pacchetti di regole per rilevare e segnalare il codice che viola le best practice. Per ulteriori informazioni sulle regole e un elenco completo, vedete cdk-nag rules (). GitHub

Politica personalizzata di minimo privilegio per il ruolo di distribuzione AWS CDK

ADDF fa ampio uso della versione 2. AWS CDK È necessario eseguire il bootstrap di tutti gli ADDF su. Account AWS AWS CDK Per ulteriori informazioni, consulta Bootstrapping (Processo di bootstrap) (documentazione AWS CDK).

Per impostazione predefinita, AWS CDK assegna la politica AdministratorAccess AWS gestita permissiva al ruolo di AWS CDK distribuzione creato negli account avviati. Il nome completo di

questo ruolo è. `cdk-[CDK_QUALIFIER]-cfn-exec-role-[AWS_ACCOUNT_ID]-[REGION]` AWS CDK utilizza questo ruolo per distribuire risorse nel sistema bootstrap Account AWS come parte del AWS CDK processo di distribuzione.

A seconda dei requisiti di sicurezza dell'organizzazione, la policy `AdministratorAccess` potrebbe essere troppo permissiva. Come parte del processo di bootstrap di AWS CDK , è possibile personalizzare la policy e le autorizzazioni in base a esigenze specifiche. È possibile modificare la policy sottoponendo nuovamente l'account a bootstrap con una policy appena definita utilizzando il parametro `--cloudformation-execution-policies`. Per ulteriori informazioni, consulta Personalizzazione del bootstrap (documentazione).AWS CDK

> **Note**
>
> Sebbene questa funzionalità di sicurezza non sia specifica dell'ADDF, è stata inserita in questa sezione perché può aumentare la sicurezza complessiva dell'implementazione dell'ADDF.

Policy del privilegio minimo per il file deployspec del modulo

Ogni modulo contiene un file delle specifiche di implementazione denominato deployspec.yaml. Questo file definisce le istruzioni di distribuzione per il modulo. CodeSeeder lo usa per distribuire il modulo definito nell'account di destinazione utilizzando AWS CodeBuild. CodeSeeder assegna un ruolo di servizio predefinito CodeBuild alla distribuzione delle risorse, come indicato nel file delle specifiche di distribuzione. Questo ruolo di servizio è progettato secondo il principio del privilegio minimo. Include tutte le autorizzazioni necessarie per distribuire le AWS CDK applicazioni, poiché tutti i moduli forniti da ADDF vengono creati come applicazioni. AWS CDK

Tuttavia, se è necessario eseguire comandi di stage all'esterno di AWS CDK, è necessario creare una policy IAM personalizzata anziché utilizzare il ruolo di servizio predefinito per. CodeBuild Ad esempio, se si utilizza un framework di distribuzione IaC diverso da AWS CDK, come Terraform, è necessario creare una policy IAM che conceda autorizzazioni sufficienti per il funzionamento di quel framework specifico. Un altro scenario che richiede una policy IAM dedicata è quando si includono chiamate direct AWS Command Line Interface (AWS CLI) ad altri comandi Servizi AWS in`install`, `pre_build`build, o stage. `post_build` Ad esempio, è necessaria una policy personalizzata se il modulo include un comando Amazon Simple Storage Service (Amazon S3) per caricare file in un bucket S3. La policy IAM personalizzata fornisce un controllo granulare per qualsiasi AWS comando

al di fuori della distribuzione. AWS CDK Quando crei una policy IAM personalizzata per il tuo modulo ADDF, assicurati di applicare le autorizzazioni con privilegi minimi.

Crittografia dei dati

L'ADDF archivia ed elabora dati potenzialmente sensibili. Per contribuire alla protezione di questi dati SeedFarmer CodeSeeder, i moduli forniti da ADDF crittografano i dati inattivi e in transito per tutti gli utenti utilizzati Servizi AWS (salvo diversa indicazione esplicita per i moduli nella cartella). `demo-only`

Archiviazione delle credenziali tramite Secrets Manager

ADDF gestisce vari segreti per diversi servizi, come Docker Hub e Amazon JupyterHub Redshift. L'ADDF usa Gestione dei segreti AWS per memorizzare tutti i segreti relativi all'ADDF stesso. Questo aiuta a rimuovere i dati sensibili dal codice sorgente.

I segreti di Secrets Manager vengono archiviati solo negli account di destinazione e nella misura necessaria per il corretto funzionamento dell'account. Per impostazione predefinita, l'account toolchain non contiene segreti.

Recensioni di sicurezza di e SeedFarmer CodeSeeder

SeedFarmere CodeSeeder(GitHubrepository) vengono utilizzati per distribuire ADDF e i relativi moduli ADDF. Questi progetti open source sono sottoposti allo stesso normale processo di revisione della sicurezza AWS interna di ADDF, come descritto in. Processo di revisione della sicurezza dell'ADDF

Autorizzazioni, limiti, supporto per il ruolo di AWS CodeBuild CodeSeeder

I limiti delle autorizzazioni IAM sono un meccanismo di sicurezza comune che definisce le autorizzazioni massime che una policy basata sull'identità può concedere a un'entità IAM. SeedFarmer e CodeSeeder supportano un allegato ai limiti delle autorizzazioni IAM per ogni account di destinazione. Il limite delle autorizzazioni limita le autorizzazioni massime di qualsiasi ruolo di servizio utilizzato da quando distribuisce i moduli. CodeBuild CodeSeeder I limiti delle autorizzazioni IAM devono essere creati da un team di sicurezza al di fuori dell'ADDF. Gli allegati della policy per

impostare il limite delle autorizzazioni IAM sono accettati come attributo all'interno del file manifesto dell'implementazione dell'ADDF, deployment.yaml. Per ulteriori informazioni, consulta Limiti delle autorizzazioni (documentazione). SeedFarmer

Di seguito è riportato il flusso di lavoro:

1. Il tuo team di sicurezza definisce e crea un limite delle autorizzazioni IAM in base ai tuoi requisiti di sicurezza. Il limite delle autorizzazioni IAM deve essere creato individualmente in ogni ADDF. Account AWS L'output è un elenco del nome della risorsa Amazon (ARN) per una policy per impostare il limite delle autorizzazioni.
2. Il team addetto alla sicurezza condivide l'elenco dell'ARN per la policy con il team di sviluppatori ADDF.
3. Il team di sviluppatori ADDF integra l'elenco dell'ARN per le policy nel file manifesto. Per un esempio di questa integrazione, vedete sample-permissionboundary.yaml (). GitHub
4. Dopo una corretta implementazione, il limite delle autorizzazioni viene collegato a tutti i ruoli di servizio utilizzati per distribuire i moduli. CodeBuild
5. Il team di sicurezza controlla che i limiti delle autorizzazioni vengano applicati in base alle necessità.

AWS architettura multi-account

Come definito nel pilastro della sicurezza del AWS Well-Architected Framework, è considerata una buona pratica separare le risorse e i carichi di lavoro in Account AWS più, in base ai requisiti dell'organizzazione. Questo perché un Account AWS funge da confine di isolamento. Per ulteriori informazioni, consulta gestione e separazione degli Account AWS. L'implementazione di questo concetto si chiama architettura multi-account. Un'architettura AWS multi-account correttamente progettata fornisce una categorizzazione del carico di lavoro e riduce la portata dell'impatto in caso di violazione della sicurezza rispetto a un'architettura ad account singolo.

ADDF supporta nativamente architetture multi-account AWS . Puoi distribuire i tuoi moduli ADDF su tutti quelli necessari per la sicurezza e Account AWS i requisiti della tua organizzazione. separation-of-duties È possibile implementare l'ADDF in un unico Account AWS, combinando le funzioni dell'account toolchain e dell'account di destinazione. In alternativa, è possibile creare account di destinazione individuali per i moduli o i gruppi di moduli ADDF.

L'unica restrizione da considerare è che un modulo ADDF rappresenta l'unità di distribuzione più piccola per ciascuno di essi. Account AWS

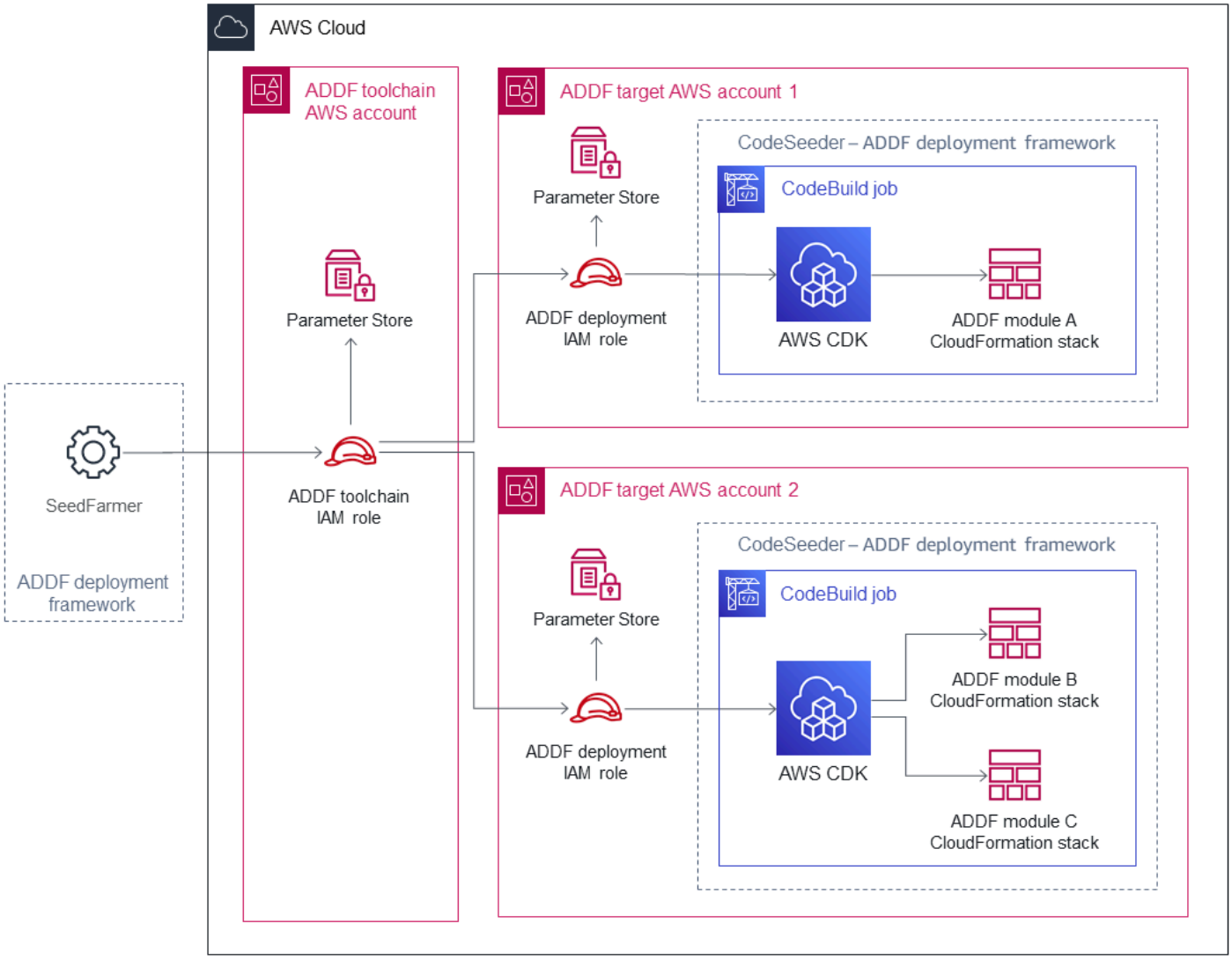
Per gli ambienti di produzione, si consiglia di utilizzare un'architettura multi-account composta da un account toolchain e almeno un account di destinazione. Per ulteriori informazioni, consulta Architettura dell'ADDF.

Autorizzazioni con privilegi minimi per e implementazioni multi-account

Se si utilizza un'architettura multi-account, è SeedFarmer necessario accedere agli account di destinazione per eseguire le seguenti tre azioni:

1. Scrivere i metadati del modulo ADDF nell'account toolchain e negli account di destinazione.
2. Leggere i metadati del modulo ADDF correnti dall'account toolchain e dagli account di destinazione.
3. Avvia AWS CodeBuild processi negli account di destinazione, allo scopo di distribuire o aggiornare i moduli.

La figura seguente mostra le relazioni tra account, incluse le operazioni per l'assunzione di ruoli specifici per ADDF AWS Identity and Access Management (IAM).



Queste operazioni tra account vengono realizzate utilizzando operazioni di assume-role ben definite.

- Il ruolo IAM della toolchain ADDF viene distribuito nell'account della toolchain. SeedFarmer assume questo ruolo. Questo ruolo dispone delle autorizzazioni per eseguire un'operazione di `iam:AssumeRole` e può assumere il ruolo IAM di implementazione dell'ADDF in ogni account di destinazione. Inoltre, il ruolo IAM della toolchain ADDF può eseguire operazioni locali di AWS Systems Manager Parameter Store.
- Il ruolo IAM di implementazione dell'ADDF viene implementato in ogni account di destinazione. Questo ruolo può essere assunto solo dall'account toolchain usando il ruolo IAM toolchain ADDF. Questo ruolo dispone delle autorizzazioni per eseguire operazioni locali di AWS Systems Manager Parameter Store e dispone delle autorizzazioni per eseguire AWS CodeBuild azioni che avviano e descrivono i lavori. CodeBuild CodeSeeder

Questi ruoli IAM specifici per l'ADDF vengono creati come parte del processo di bootstrap dell'ADDF. Per ulteriori informazioni, vedete Bootstrap Account AWS(s) nella ADDF Deployment Guide (). GitHub

Tutte le autorizzazioni tra più account sono impostate in base al principio del privilegio minimo. Se un account di destinazione viene compromesso, l'impatto sull'altro Account AWS ADDF è minimo o nullo.

Nel caso di un'architettura ad account singolo per l'ADDF, le relazioni tra i ruoli rimangono le stesse, ma si riuniscono in un unico Account AWS.

Configurazione e funzionamento sicuri dell'ADDF

Autonomous Driving Data Framework (ADDF) deve essere trattato come un software personalizzato che richiede manutenzione e assistenza continue da parte di un team dedicato DevOps e addetto alla sicurezza dell'organizzazione. Questa sezione descrive le attività relative alla sicurezza comuni che consentono di configurare e utilizzare l'ADDF per tutto il suo ciclo di vita.

Questa sezione contiene le attività seguenti:

- Definizione dell'architettura dell'ADDF
- Configurazione iniziale dell’
- Personalizzazione del codice del framework di implementazione ADDF
- Scrivere moduli personalizzati nell'ADDF
- Implementazioni ADDF ricorrenti
- Controlli di sicurezza ricorrenti
- Aggiornamenti dell'ADDF
- Disattivazione

Definizione dell'architettura dell'ADDF

Un'istanza ADDF è sicura solo quanto l' Account AWS ambiente in cui è distribuita. Questo Account AWS ambiente deve essere progettato per soddisfare le esigenze operative e di sicurezza del caso d'uso specifico. Ad esempio, le attività e le considerazioni relative alla sicurezza e alle operazioni per la configurazione di un'istanza ADDF in un ambiente proof-of-concept (PoC) sono diverse da quelle per la configurazione di ADDF in un ambiente di produzione.

Esecuzione dell'ADDF in un ambiente PoC

Se intendi utilizzare ADDF in un ambiente PoC, ti consigliamo di crearne uno dedicato Account AWS per ADDF che non contenga altri carichi di lavoro. Questo aiuta a proteggere il tuo account mentre esplori l'ADDF e le sue funzionalità. I vantaggi di questo approccio sono i seguenti:

- In caso di gravi errori di configurazione dell'ADDF, nessun altro carico di lavoro subirebbe conseguenze negative.

- Non c'è il rischio di altre configurazioni del carico di lavoro errate che potrebbero influire negativamente sulla configurazione dell'ADDF.

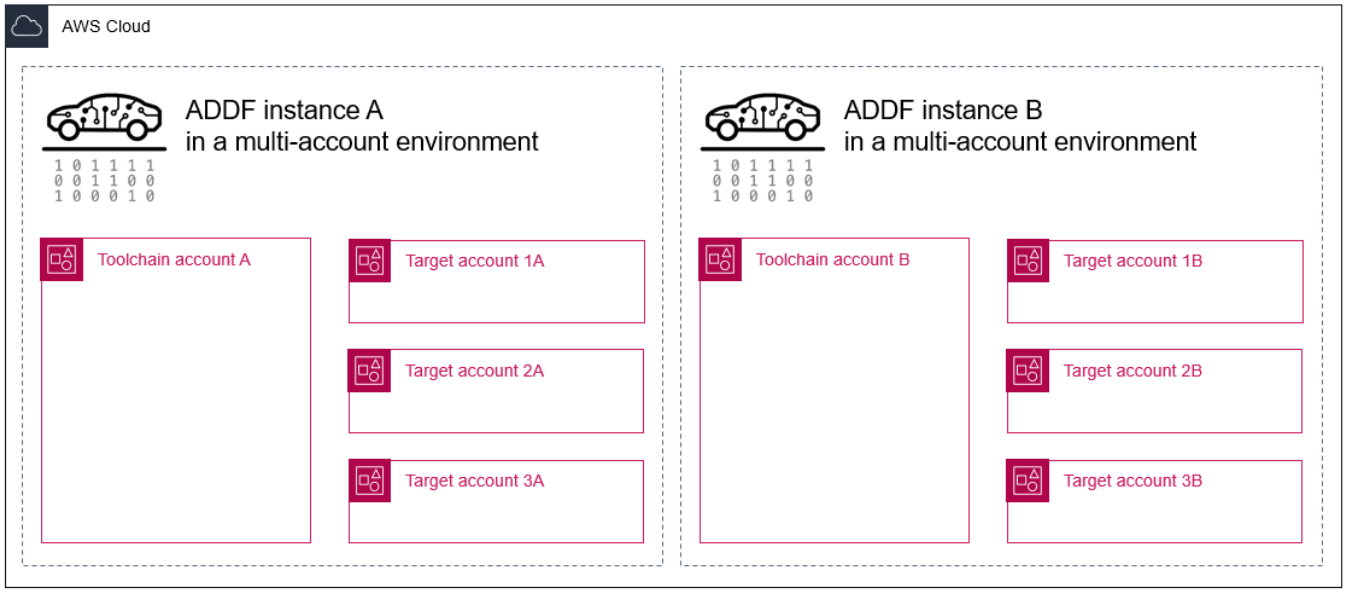
Anche per l'ambiente PoC, è comunque preferibile seguire il più possibile tutte le best practice elencate in Esecuzione dell'ADDF in un ambiente di produzione.

Esecuzione dell'ADDF in un ambiente di produzione

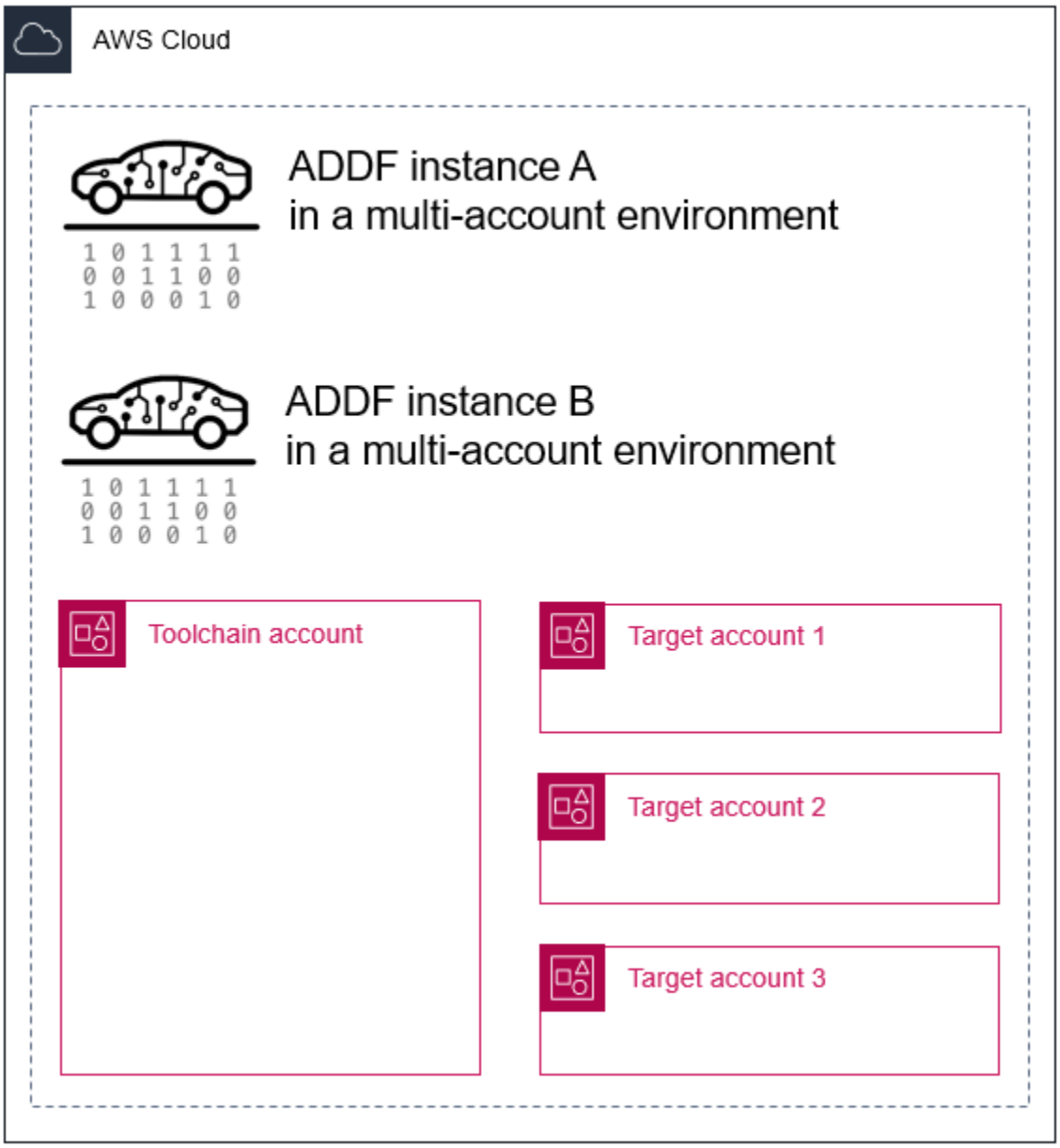
Se intendi utilizzare ADDF in un ambiente di produzione aziendale, ti consigliamo vivamente di osservare le best practice di sicurezza della tua organizzazione e di implementare l'ADDF di conseguenza. Oltre a seguire le best practice di sicurezza della tua organizzazione, ti consigliamo di adottare i seguenti accorgimenti:

- Crea un DevOps team ADDF impegnato a lungo termine: ADDF deve essere trattato come un software personalizzato. Richiede manutenzione e assistenza continue da parte di un team dedicato DevOps. Prima di iniziare a eseguire ADDF in un ambiente di produzione, è necessario definire un DevOps team di dimensioni e capacità sufficienti con un impegno completo di risorse, fino alla distribuzione end-of-life di ADDF.
- Utilizza un'architettura multi-account: ciascuna istanza ADDF deve essere implementata nel proprio ambiente AWS multi-account dedicato, senza altri carichi di lavoro non correlati. Come definito nella gestione e separazione degli AWS account (AWS Well-Architected Framework), è considerata una buona pratica separare le risorse e i carichi di lavoro in Account AWS più, in base ai requisiti dell'organizzazione. Questo perché un Account AWS funge da confine di isolamento. Un'architettura AWS multi-account correttamente progettata fornisce una categorizzazione del carico di lavoro e riduce la portata dell'impatto in caso di violazione della sicurezza rispetto a un'architettura ad account singolo. L'utilizzo di un'architettura multi-account aiuta inoltre gli account a restare all'interno delle loro quote Servizio AWS. Distribuisci i moduli ADDF tra tutti Account AWS quelli necessari per soddisfare i requisiti di sicurezza e separation-of-duties di sicurezza dell'organizzazione.
- Implementa più istanze ADDF: configura tutte le istanze ADDF separate di cui hai bisogno per sviluppare, testare e implementare correttamente i moduli ADDF in base ai processi di sviluppo software della tua organizzazione. Inoltre, quando configuri più istanze ADDF puoi utilizzare uno dei seguenti approcci:
  - Più istanze ADDF in diversi ambienti con AWS più account: puoi usarle separate Account AWS per isolare diverse istanze ADDF. Ad esempio, se l'organizzazione ha fasi di sviluppo, test e produzione dedicate, è possibile creare istanze ADDF separate e account dedicati per ogni fase.

Ciò offre molti vantaggi, quali la riduzione del rischio di propagazione degli errori tra più fasi, e aiuta a implementare un processo di approvazione e a limitare l'accesso degli utenti solo a determinati ambienti. L'immagine seguente mostra due istanze ADDF implementate in ambienti multi-account separati.



- Più istanze ADDF nello stesso ambiente AWS multi-account: puoi creare più istanze ADDF che condividono lo stesso ambiente multi-account. AWS Questo crea efficacemente rami isolati negli stessi Account AWS. Ad esempio, se diversi sviluppatori lavorano in parallelo, uno sviluppatore può creare un'istanza ADDF dedicata negli stessi Account AWS. Questo aiuta gli sviluppatori a lavorare in rami isolati per scopi di sviluppo e test. Se si utilizza questo approccio, le risorse ADDF devono avere nomi di risorse univoci per ogni istanza ADDF. Per impostazione predefinita, questa funzionalità è supportata nei moduli forniti di default dall'ADDF. È possibile utilizzare questo approccio purché non si superino le quote Servizio AWS. L'immagine seguente mostra due istanze ADDF implementate in un ambiente multi-account condiviso.



- Istanze ADDF multiple nello stesso ambiente AWS ad account singolo - Questa architettura è molto simile all'esempio precedente. La differenza sta nel fatto che le istanze ADDF multiple vengono implementate in un ambiente ad account singolo invece che in un ambiente multi-account. Questa architettura può adattarsi a casi d'uso dell'ADDF molto semplici caratterizzati da un ambito molto limitato e con più sviluppatori che lavorano contemporaneamente su diversi rami.

Poiché SeedFarmer è l'unico strumento che controlla le distribuzioni di un'istanza ADDF, puoi creare qualsiasi ambiente e architettura di account che si adatti alla strategia e ai processi di distribuzione della tua organizzazione. CI/CD

- Personalizza il processo di AWS Cloud Development Kit (AWS CDK) bootstrap in base ai requisiti di sicurezza dell'organizzazione: per impostazione predefinita, AWS CDK assegna la policy AdministratorAccess AWS gestita durante il processo di avvio. Inoltre, questa policy garantisce privilegi amministrativi completi. Se questa policy è troppo permissiva per i requisiti di sicurezza dell'organizzazione, è possibile personalizzare i criteri da applicare. Per ulteriori informazioni, consulta Politica personalizzata di minimo privilegio per il ruolo di distribuzione AWS CDK.
- Rispetta le migliori pratiche durante la configurazione dell'accesso in IAM: crea una soluzione di accesso strutturata AWS Identity and Access Management (IAM) che consenta agli utenti di accedere all'ADDF. Account AWS L'ADDF è progettato per aderire al principio del privilegio minimo. Il tuo schema di accesso IAM dovrebbe inoltre seguire il principio del privilegio minimo, essere conforme ai requisiti dell'organizzazione e rispettare le best practice per la sicurezza in IAM (documentazione IAM).

- Configura la rete secondo le best practice della tua organizzazione: ADDF include uno stack AWS CloudFormation di rete opzionale che crea un cloud privato virtuale (VPC) pubblico o privato di base. A seconda della configurazione dell'organizzazione, questo VPC potrebbe esporre le risorse direttamente a Internet. Pertanto ti consigliamo di seguire le best practice di rete della tua organizzazione e di creare un modulo di rete personalizzato con protezione avanzata.
- Implementa misure di prevenzione, rilevamento e mitigazione della sicurezza a Account AWS livello: AWS offre vari servizi di sicurezza, come Amazon GuardDuty, AWS Security Hub CSPM Amazon Detective e. AWS Config Abilita questi servizi nel tuo ADDF Account AWS e integra i processi di prevenzione, rilevamento, mitigazione e gestione degli incidenti di sicurezza della tua organizzazione. È fortemente consigliato seguire le Best practice per sicurezza, identità e conformità (Centro di architettura AWS) ed eventuali raccomandazioni specifiche relative al servizio contenute nella documentazione relativa a tale servizio. Per ulteriori informazioni, consulta la Documentazione sulla sicurezza AWS.

L'ADDF non affronta nessuno di questi argomenti perché i dettagli di implementazione e configurazione dipendono in larga misura dai requisiti e dai processi specifici dell'organizzazione. Affrontare questi argomenti è invece una responsabilità fondamentale dell'organizzazione. In genere, il team che gestisce la zona di destinazione AWS può aiutarti a pianificare e implementare il tuo ambiente ADDF.

Configurazione iniziale dell’

Configura ADDF in base alla ADDF Deployment Guide (). GitHub Il punto di partenza per qualsiasi implementazione è la `/manifest` cartella nell'archivio autonomous-driving-data-frameworkGit Hub. La cartella `/manifest/example-dev` contiene un'implementazione di esempio a scopo dimostrativo. Puoi usare questo esempio come punto di partenza per progettare la tua implementazione. In quella directory è presente un file manifesto dell'implementazione dell'ADDF chiamato deployment.yaml. Contiene tutte le informazioni per SeedFarmer gestire, distribuire o eliminare ADDF e le relative risorse in. Cloud AWSÈ possibile creare gruppi di moduli ADDF in file dedicati. Il file core-modules.yaml è un esempio del gruppo di moduli core e include tutti i moduli principali forniti dall'ADDF. Per riassumere, il file deployment.yaml contiene tutti i riferimenti ai gruppi e ai moduli che saranno implementati nei rispettivi account di destinazione e specifica l'ordine di implementazione.

Per una configurazione sicura e conforme, soprattutto in un ambiente che non è un proof of concept, si consiglia di esaminare il codice sorgente di ogni modulo da implementare. In base alle best

practice di rafforzamento della sicurezza, è preferibile implementare solo i moduli necessari per il caso d'uso previsto.

> **Note**
>
> I moduli ADDF nella cartella `modules/demo-only/` non hanno una sicurezza elevata e non dovrebbero essere implementati in ambienti di produzione o in qualsiasi ambiente con dati sensibili o protetti. Questi moduli sono inclusi per mostrare le funzionalità del sistema e possono essere utilizzati come base per creare moduli personalizzati e dotati di protezione avanzata.

Personalizzazione del codice del framework di implementazione ADDF

Il framework di implementazione ADDF e la sua logica di orchestrazione e implementazione possono essere completamente personalizzati per soddisfare qualsiasi esigenza. Tuttavia, ti consigliamo di astenerti dal personalizzarlo o di ridurre le modifiche al minimo per i seguenti motivi:

- Mantenere la compatibilità upstream: la compatibilità upstream semplifica l'aggiornamento dell'ADDF per le funzionalità e gli aggiornamenti di sicurezza più recenti. La modifica del framework interrompe la retrocompatibilità nativa con e con tutti SeedFarmer i CodeSeeder moduli principali ADDF.
- Conseguenze sulla sicurezza: la modifica del framework di implementazione ADDF può essere un'attività complessa che può avere conseguenze indesiderate sulla sicurezza. Nel peggiore dei casi, le modifiche al framework possono causare vulnerabilità per la sicurezza.

Quando possibile, crea e personalizza il codice del tuo modulo invece di modificare il framework di implementazione ADDF e il codice del modulo ADDF principale.

> **Note**
>
> Se ritieni che parti specifiche del framework di implementazione ADDF necessitino di miglioramenti o di un ulteriore rafforzamento della sicurezza, apporta le tue modifiche al repository ADDF tramite una richiesta pull. Per ulteriori informazioni, consulta Revisioni e contributi open source sulla sicurezza.

Scrivere moduli personalizzati nell'ADDF

La creazione di un nuovo modulo ADDF o l'estensione di un modulo esistente è un concetto fondamentale dell'ADDF. Quando crei o personalizzi i moduli, ti suggeriamo di seguire le best practice generali di sicurezza di AWS e le best practice della tua organizzazione per una codifica sicura. Inoltre, per ridurre ulteriormente il rischio di problemi di sicurezza, si consiglia di effettuare revisioni tecniche di sicurezza sia iniziali che periodiche, interne o esterne, in base ai requisiti di sicurezza dell'organizzazione.

Implementazioni ADDF ricorrenti

Implementate ADDF e i relativi moduli come descritto nella Guida alla distribuzione di ADDF (). GitHub Per supportare le distribuzioni ADDF ricorrenti che aggiungono, aggiornano o rimuovono risorse negli account di destinazione, SeedFarmer utilizza gli MD5 hash, memorizzati nell'archivio dei parametri della toolchain e degli account di destinazione, per confrontare l'infrastruttura attualmente distribuita con l'infrastruttura definita nei file manifest nella base di codice locale.

Questo approccio segue il GitOps paradigma, in cui il repository di origine (la base di codice locale in cui si opera SeedFarmer) è la fonte della verità e l'infrastruttura dichiarata esplicitamente in esso è il risultato desiderato della distribuzione. Per ulteriori informazioni su GitOps, consulta What is GitOps (GitLab sito Web).

Controlli di sicurezza ricorrenti

Proprio come per qualsiasi altro software della tua organizzazione, integra l'ADDF e il codice del modulo ADDF personalizzato nella gestione dei rischi di sicurezza, nella revisione della sicurezza e nel ciclo di audit di sicurezza.

Aggiornamenti dell'ADDF

L'ADDF riceve aggiornamenti regolari come parte del suo continuo impegno nello sviluppo. Ciò include aggiornamenti delle funzionalità e miglioramenti e correzioni in termini di sicurezza. Ti consigliamo di controllare regolarmente la presenza di nuove versioni del framework e di applicare gli aggiornamenti tempestivamente. Per ulteriori informazioni, consulta Procedura per aggiornare l'ADDF (Documentazione ADDF).

Disattivazione

Se l'ADDF non è più necessario, elimina l'ADDF e tutte le risorse correlate dai tuoi Account AWS. Qualsiasi infrastruttura non presidiata e non utilizzata comporta costi inutili e rappresenta un potenziale rischio per la sicurezza. Per ulteriori informazioni, consulta Passaggi per eliminare ADDF in modo definitivo (Documentazione ADDF).

Passaggi successivi

Questa guida ha esaminato le migliori pratiche e considerazioni relative alla sicurezza e alle operazioni durante l'implementazione dell'Autonomous Driving Data Framework (ADDF) nell'ambiente in uso. Cloud AWS Questa guida esamina il modello di responsabilità condivisa tra l'utente ADDF e il team principale di ADDF, in AWS modo da comprendere il ruolo e le responsabilità dell'utente nell'impostare e utilizzare ADDF in modo sicuro. Sono anche incluse alcune raccomandazioni per utilizzare l'ADDF in modo sicuro durante tutto il suo ciclo di vita, con indicazioni specifiche per l'ambiente.

Si consiglia di acquisire familiarità con le risorse disponibili nella sezione Risorse. Quando sei pronto, puoi configurare ADDF seguendo le istruzioni contenute nella ADDF Deployment Guide (). GitHub

Durante la configurazione e l'utilizzo di ADDF, se ritieni che il framework di implementazione necessiti di miglioramenti o di un ulteriore rafforzamento della sicurezza, contribuisci con le tue modifiche al repository ADDF tramite una richiesta pull. Per ulteriori informazioni, consulta Revisioni e contributi open source sulla sicurezza.

Risorse

AWS documentazione

- Sviluppa e implementa un flusso di lavoro personalizzato utilizzando ADDF su AWS (AWS post del blog)
- AWS documentazione sul servizio di sicurezza
- Best practice per la sicurezza in IAM
- AWS gestione e separazione degli account
- Bootstrap per AWS CDK
- Modello di responsabilità condivisa di AWS
- AWS Well-Architected Framework

Risorse open source

- Archivio ADDF () GitHub
- Guida alla distribuzione di ADDF () GitHub
- CodeSeederarchivio () GitHub
- SeedFarmerdeposito () GitHub

Note

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

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

Cronologia dei documenti

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

Modifica	Descrizione	Data
Pubblicazione iniziale	—	15 novembre 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 tuo database Oracle locale a Oracle su un'istanza EC2 in. Cloud AWS
- Trasferire (eseguire il rehosting a livello hypervisor): trasferisci l'infrastruttura sul cloud senza acquistare nuovo hardware, riscrivere le applicazioni o modificare le operazioni esistenti. Esegui la migrazione dei server da una piattaforma locale a un servizio cloud per la stessa piattaforma. Esempio: migra un'applicazione suMicrosoft Hyper-V. AWS
- Riesaminare (mantenere): mantieni le applicazioni nell'ambiente di origine. Queste potrebbero includere applicazioni che richiedono una rifattorizzazione significativa che desideri rimandare a un momento successivo e applicazioni legacy che desideri mantenere, perché non vi è alcuna giustificazione aziendale per effettuarne la migrazione.
- Ritirare: disattiva o rimuovi le applicazioni che non sono più necessarie nell'ambiente di origine.

A

ABAC

Vedi controllo degli accessi basato sugli attributi.

servizi astratti

Vedi servizi gestiti.

ACIDO

Vedi atomicità, consistenza, isolamento, durata.

migrazione attiva-attiva

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

migrazione attiva-passiva

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

funzione di aggregazione

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

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

controllo delle applicazioni

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

portfolio di applicazioni

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

intelligenza artificiale (IA)

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

operazioni di intelligenza artificiale (AIOps)

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

crittografia asimmetrica

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

atomicità, consistenza, isolamento, durabilità (ACID)

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

Controllo degli accessi basato su attributi (ABAC)

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

fonte di dati autorevole

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

Zona di disponibilità

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

AWS Cloud Adoption Framework (CAF)AWS

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

AWS Workload Qualification Framework (WQF)AWS

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

B

bot difettoso

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

BCP

Vedi la pianificazione della continuità operativa.

grafico comportamentale

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

sistema big-endian

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

Classificazione binaria

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

filtro Bloom

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

implementazione blu/verde

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

bot

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

botnet

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

ramo

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

accesso break-glass

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

strategia brownfield

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

cache del buffer

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

capacità di business

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

pianificazione della continuità operativa (BCP)

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

C

CAF

Vedi Cloud Adoption AWS Framework.

implementazione canaria

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

CCoE

Vedi Cloud Center of Excellence.

CDC

Vedi Change Data Capture.

Change Data Capture (CDC)

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

ingegneria del caos

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

CI/CD

Vedi integrazione continua e distribuzione continua.

classificazione

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

crittografia lato client

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

Centro di eccellenza cloud (CCoE)

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

cloud computing

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

modello operativo cloud

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

fasi di adozione del cloud

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

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

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

CMDB

Vedi database di gestione della configurazione.

repository di codice

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

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

cache fredda

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

dati freddi

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

visione artificiale (CV)

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

deriva della configurazione

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

database di gestione della configurazione (CMDB)

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

Pacchetto di conformità

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

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

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

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

CV

Vedi visione artificiale.

D

dati a riposo

Dati stazionari nella rete, ad esempio i dati archiviati.

classificazione dei dati

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

deriva dei dati

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

dati in transito

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

rete di dati

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

riduzione al minimo dei dati

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

perimetro dei dati

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

pre-elaborazione dei dati

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

provenienza dei dati

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

soggetto dei dati

Un individuo i cui dati vengono raccolti ed elaborati.

data warehouse

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

linguaggio di definizione del database (DDL)

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

linguaggio di manipolazione del database (DML)

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

DDL

Vedi linguaggio di definizione del database.

deep ensemble

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

deep learning

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

defense-in-depth

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

amministratore delegato

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

implementazione

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

Ambiente di sviluppo

Vedi ambiente.

controllo di rilevamento

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

mappatura del flusso di valore dello sviluppo (DVSM)

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

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

gemello digitale

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

tabella delle dimensioni

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

disastro

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

disaster recovery (DR)

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

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

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

DOTT.

Vedi disaster recovery.

rilevamento della deriva

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

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

MODIFICA

Vedi scambio elettronico di dati.

edge computing

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

scambio elettronico di dati (EDI)

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

crittografia

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

chiave crittografica

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

endianità

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

endpoint

Vedi service endpoint.

servizio endpoint

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

pianificazione delle risorse aziendali (ERP)

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

crittografia envelope

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

ambiente

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

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

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

epica

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

ERP

Vedi pianificazione delle risorse aziendali.

analisi esplorativa dei dati (EDA)

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

F

tabella dei fatti

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

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

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

prompt con pochi scatti

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

Vedi modello di base.

modello di fondazione (FM)

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

G

IA generativa

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

blocco geografico

Vedi restrizioni geografiche.

limitazioni geografiche (blocco geografico)

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

Flusso di lavoro di GitFlow

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

immagine dorata

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

strategia greenfield

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

guardrail

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

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

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

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

alta disponibilità (HA)

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

modernizzazione storica

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

dati di blocco

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

migrazione di database omogenea

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

dati caldi

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

hotfix

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

periodo di hypercare

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

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

I

IaC

Vedi l'infrastruttura come codice.

Policy basata su identità

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

applicazione inattiva

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

IIoT

Vedi Industrial Internet of Things.

infrastruttura immutabile

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

VPC in ingresso (ingress)

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

migrazione incrementale

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

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

IIoInternet delle cose industriale (T)

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

VPC di ispezione

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

Internet of Things (IoT)

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

interpretabilità

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

IoT

Vedi Internet of Things.

libreria di informazioni IT (ITIL)

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

gestione dei servizi IT (ITSM)

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

ITIL

Vedi la libreria di informazioni IT.

ITSM

Vedi Gestione dei servizi IT.

L

controllo degli accessi basato su etichette (LBAC)

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

zona di destinazione

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

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

modello linguistico di grandi dimensioni (LLM)

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

migrazione su larga scala

Una migrazione di 300 o più server.

BIANCO

Vedi controllo degli accessi basato su etichette.

Privilegio minimo

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

eseguire il rehosting (lift and shift)

Vedi 7 R.

sistema little-endian

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

LLM

Vedi modello linguistico di grandi dimensioni.

ambienti inferiori

Vedi ambiente.

M

machine learning (ML)

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

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

ramo principale

Vedi filiale.

malware

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

servizi gestiti

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

sistema di esecuzione della produzione (MES)

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

MAP

Vedi Migration Acceleration Program.

meccanismo

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

account membro

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

MEH

Vedi sistema di esecuzione della produzione.

Message Queuing Telemetry Transport (MQTT)

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

microservizio

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

architettura di microservizi

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

Programma di accelerazione della migrazione (MAP)

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

migrazione su larga scala

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

fabbrica di migrazione

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

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

metadati di migrazione

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

modello di migrazione

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

Valutazione del portfolio di migrazione (MPA)

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

valutazione della preparazione alla migrazione (MRA)

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

strategia di migrazione

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

ML

Vedi machine learning.

modernizzazione

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

valutazione della preparazione alla modernizzazione

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

applicazioni monolitiche (monoliti)

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

MAPPA

Vedi Migration Portfolio Assessment.

MQTT

Vedi Message Queuing Telemetry Transport.

classificazione multiclasse

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

infrastruttura mutabile

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

O

OAC

Vedi Origin Access Control.

QUERCIA

Vedi Origin Access Identity.

OCM

Vedi gestione delle modifiche organizzative.

migrazione offline

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

OI

Vedi l'integrazione delle operazioni.

OLA

Vedi accordo a livello operativo.

migrazione online

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

OPC-UA

Vedi Open Process Communications - Unified Architecture.

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

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

accordo a livello operativo (OLA)

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

revisione della prontezza operativa (ORR)

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

tecnologia operativa (OT)

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

integrazione delle operazioni (OI)

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

trail organizzativo

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

gestione del cambiamento organizzativo (OCM)

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

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

controllo dell'accesso all'origine (OAC)

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

identità di accesso origine (OAI)

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

ORR

Vedi la revisione della prontezza operativa.

NON

Vedi la tecnologia operativa.

VPC in uscita (egress)

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

P

limite delle autorizzazioni

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

informazioni di identificazione personale (PII)

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

Informazioni che consentono l'identificazione personale degli utenti

Visualizza le informazioni di identificazione personale.

playbook

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

PLC

Vedi controllore logico programmabile.

PLM

Vedi la gestione del ciclo di vita del prodotto.

policy

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

persistenza poliglotta

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

valutazione del portfolio

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

predicate

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

predicato pushdown

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

controllo preventivo

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

principale

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

privacy fin dalla progettazione

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

zone ospitate private

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

controllo proattivo

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

gestione del ciclo di vita del prodotto (PLM)

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

Ambiente di produzione

Vedi ambiente.

controllore logico programmabile (PLC)

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

concatenamento rapido

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

pseudonimizzazione

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

publish/subscribe (pub/sub)

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

Q

Piano di query

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

regressione del piano di query

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

R

Matrice RACI

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

RAG

Vedi Retrieval Augmented Generation.

ransomware

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

Matrice RASCI

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

RCAC

Vedi controllo dell'accesso a righe e colonne.

replica di lettura

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

riprogettare

Vedi 7 Rs.

obiettivo del punto di ripristino (RPO)

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

obiettivo del tempo di ripristino (RTO)

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

rifattorizzare

Vedi 7 R.

Region

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

regressione

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

riospitare

Vedi 7 R.

rilascio

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

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

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

policy basata su risorse

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

matrice di assegnazione di responsabilità (RACI)

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

controllo reattivo

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

retain

Vedi 7 R.

andare in pensione

Vedi 7 Rs.

Retrieval Augmented Generation (RAG)

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

rotazione

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

controllo dell'accesso a righe e colonne (RCAC)

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

RPO

Vedi obiettivo del punto di ripristino.

VERSO

Vedi obiettivo del tempo di ripristino.

runbook

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

S

SAML 2.0

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

SCADA

Vedi controllo di supervisione e acquisizione dati.

SCP

Vedi la politica di controllo del servizio.

Secret

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

sicurezza fin dalla progettazione

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

controllo di sicurezza

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

rafforzamento della sicurezza

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

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

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

automazione della risposta alla sicurezza

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

Crittografia lato server

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

Policy di controllo dei servizi (SCP)

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

endpoint del servizio

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

accordo sul livello di servizio (SLA)

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

indicatore del livello di servizio (SLI)

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

obiettivo a livello di servizio (SLO)

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

Modello di responsabilità condivisa

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

SIEM

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

punto di errore singolo (SPOF)

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

SLAM

Vedi il contratto sul livello di servizio.

SLI

Vedi l'indicatore del livello di servizio.

LENTA

Vedi obiettivo del livello di servizio.

split-and-seed modello

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

SPOF

Vedi punto di errore singolo.

schema a stella

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

modello del fico strangolatore

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

sottorete

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

controllo di supervisione e acquisizione dati (SCADA)

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

crittografia simmetrica

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

test sintetici

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

prompt di sistema

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

T

tag

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

variabile di destinazione

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

elenco di attività

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

ambiente di test

Vedi ambiente.

training

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

Transit Gateway

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

flusso di lavoro basato su trunk

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

Accesso attendibile

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

regolazione

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

team da due pizze

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

U

incertezza

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

compiti indifferenziati

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

ambienti superiori

Vedi ambiente.

V

vacuum

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

controllo delle versioni

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

Peering VPC

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

vulnerabilità

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

W

cache calda

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

dati caldi

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

funzione finestra

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

Carico di lavoro

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

flusso di lavoro

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

VERME

Vedi scrivere una volta, leggere molti.

WQF

Vedi AWS Workload Qualification Framework.

scrivi una volta, leggi molte (WORM)

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

Z

exploit zero-day

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

vulnerabilità zero-day

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

prompt zero-shot

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

applicazione zombie

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

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