Implementazione di politiche per le autorizzazioni con privilegi minimi per AWS CloudFormation

AWS Linee guida prescrittive

AWS Linee guida prescrittive: Implementazione di politiche per le autorizzazioni con privilegi minimi per AWS CloudFormation

Table of Contents

Implementazione di politiche per le autorizzazioni con privilegi minimi per AWS CloudFormation

Nima Fotouhi e Moumita Saha, Amazon Web Services ()AWS

Maggio 2023 (cronologia dei documenti)

AWS CloudFormationè un servizio Infrastructure as Code (IaC) che ti aiuta a scalare lo sviluppo della tua infrastruttura cloud fornendo risorse. AWS Inoltre, ti aiuta a gestire tali risorse per tutto il loro ciclo di vita, tra e. Account AWS Regioni AWS Nel CloudFormation, si definiscono i modelli, che fungono da modello per un insieme di risorse. Si effettua quindi il provisioning di tali risorse creando e distribuendo uno stack, ovvero un gruppo di risorse correlate gestite come singola unità. È inoltre possibile utilizzare CloudFormation per distribuire set di stack, che sono gruppi di stack che è possibile creare, aggiornare ed eliminare su più account e Regioni AWS con un'unica operazione. Questa guida fornisce una panoramica su come implementare le autorizzazioni con privilegi minimi e le risorse fornite tramite. AWS CloudFormation CloudFormation

È possibile distribuire CloudFormation stack o stack set effettuando una delle seguenti operazioni:

- Accedi direttamente all' AWS ambiente tramite un principale AWS Identity and Access Management (IAM) e distribuisci gli stack. CloudFormation
- Inserisci gli CloudFormation stack in una pipeline di distribuzione e avvia l'implementazione degli stack attraverso la pipeline. La pipeline accede all' AWS ambiente tramite un principale IAM e distribuisce gli stack. Questo approccio è una best practice consigliata.

Per entrambi questi approcci, sono necessarie le autorizzazioni per distribuire CloudFormation gli stack. Ad esempio, considera un utente che intende utilizzare per CloudFormation creare un'istanza Amazon Elastic Compute Cloud (Amazon EC2). Tale istanza richiederebbe un profilo di istanza IAM per accedere ad altro. Servizi AWS Il principale IAM utilizzato per distribuire lo CloudFormation stack richiederebbe le seguenti autorizzazioni:

- Autorizzazioni di accesso CloudFormation
- Autorizzazioni per creare pile in CloudFormation
- Autorizzazioni per creare istanze in Amazon EC2
- Autorizzazioni per creare i profili di istanza IAM richiesti

Cos'è il privilegio minimo?

Il privilegio minimo è la best practice di sicurezza per la concessione delle autorizzazioni minime richieste per eseguire un'attività. Il principio del privilegio minimo fa parte del pilastro della sicurezza nel Well-Architected AWS Framework. L'implementazione di questa best practice può contribuire a proteggere AWS l'ambiente dai rischi di escalation dei privilegi, ridurre la superficie di attacco, migliorare la sicurezza dei dati e prevenire errori degli utenti (come la configurazione errata o l'eliminazione di una risorsa per errore).

Per implementare il privilegio minimo per AWS le risorse, è necessario configurare policy, come le politiche basate sull'identità in (IAM).AWS Identity and Access Management Queste politiche definiscono le autorizzazioni e specificano le condizioni di accesso. Le organizzazioni possono iniziare con policy AWS gestite, ma poi in genere creano policy personalizzate che limitano l'ambito delle autorizzazioni alle sole azioni necessarie per il carico di lavoro o il caso d'uso.

Le autorizzazioni con privilegi minimi per il servizio sono una considerazione importante in materia di sicurezza CloudFormation . Poiché gli utenti e gli sviluppatori con cui interagiscono CloudFormation possono avere la possibilità di creare, modificare o eliminare rapidamente risorse su larga scala, il privilegio minimo è particolarmente importante. Tuttavia, CloudFormation richiede le autorizzazioni necessarie per creare, aggiornare e modificare le risorse del tuo. Account AWSÈ necessario bilanciare la necessità delle autorizzazioni per funzionare CloudFormation con il principio del privilegio minimo.

Quando si applica il principio del privilegio minimo a CloudFormation, è necessario considerare quanto segue:

- Autorizzazioni per il CloudFormation servizio: a quali utenti è richiesto l'accesso CloudFormation, quale livello di accesso richiedono e quali azioni possono intraprendere per creare, aggiornare o eliminare gli stack?
- Autorizzazioni per il provisioning delle risorse: tramite quali risorse gli utenti possono effettuare il provisioning? CloudFormation
- Autorizzazioni per le risorse assegnate: come si configurano le autorizzazioni con privilegi minimi per le risorse tramite le quali si effettua il provisioning? CloudFormation

Obiettivi aziendali specifici

Seguendo le best practice e i consigli contenuti in questa guida, puoi:

- Determina a quali utenti dell'organizzazione è necessario accedere CloudFormation e quindi configura le autorizzazioni con privilegi minimi per tali utenti.
- Utilizza le policy degli stack per proteggere gli stack da aggiornamenti non intenzionali. CloudFormation
- Configura le autorizzazioni con privilegi minimi per CloudFormation utenti e risorse per prevenire l'aumento dei privilegi e il confuso problema dei vicedirettori.
- Da utilizzare per fornire risorse con autorizzazioni con privilegi minimi. AWS CloudFormation AWS Questo aiuta l'organizzazione a mantenere una posizione di sicurezza più solida.
- Riduci in modo proattivo la quantità di tempo, energia e denaro necessari per indagare e mitigare gli incidenti di sicurezza.

Destinatari principali

Questa guida è destinata agli architetti dell'infrastruttura cloud, DevOps agli ingegneri e ai tecnici dell'affidabilità dei siti (SREs) che gestiscono e forniscono risorse utilizzando. CloudFormation

Utilizzo delle politiche di accesso per concedere le autorizzazioni in AWS

Puoi gestire l'accesso AWS creando policy basate sull'identità e collegandole a principi AWS Identity and Access Management (IAM), come ruoli o utenti, e creando policy basate sulle risorse e collegandole alle risorse. AWS AWS valuta queste politiche ogni volta che viene effettuata una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta.

Per comprendere come configurare l'accesso con privilegi minimi nelle policy, è necessario comprendere i diversi tipi di policy, gli elementi e la struttura di una policy e come vengono valutate le policy. Questa guida si concentra solo sulle politiche basate sull'identità e sulle politiche basate sulle risorse. Tuttavia, AWS fornisce altri tipi di politiche, come le politiche di controllo del servizio (SCPs), i limiti delle autorizzazioni e le politiche di sessione. Ogni tipo di politica svolge un ruolo nell'implementazione delle autorizzazioni con privilegi minimi nel tuo. Account AWS Per ulteriori informazioni, consulta Politiche e autorizzazioni e Applica le autorizzazioni con privilegi minimi nella documentazione IAM.

Configurazione delle autorizzazioni con privilegi minimi da utilizzare CloudFormation

Questo capitolo esamina le opzioni per la configurazione delle autorizzazioni per accedere e utilizzare il servizio. AWS CloudFormation

Quando un utente o un servizio fornisce AWS risorse CloudFormation, il primo passaggio consiste nell'effettuare una chiamata al CloudFormation servizio tramite un preside AWS Identity and Access Management (IAM). Questo principale IAM deve disporre delle autorizzazioni per creare gli CloudFormation stack. Successivamente, il preside IAM utilizza uno dei seguenti approcci per fornire risorse tramite: CloudFormation

- Se il principale IAM non passa le operazioni dello stack a un ruolo di CloudFormation servizio, CloudFormation utilizza le credenziali del principale IAM per eseguire le operazioni dello stack. Questa è l'impostazione predefinita. Pertanto, oltre alle autorizzazioni per eseguire le operazioni di CloudFormation stack, il principale IAM necessita anche delle autorizzazioni per fornire le risorse definite nei modelli che utilizzerà. CloudFormation Ad esempio, se il responsabile IAM non dispone delle autorizzazioni per creare istanze Amazon Elastic Compute Cloud (Amazon EC2), non può CloudFormation creare uno stack per il provisioning di un'istanza Amazon EC2.
- Se il principale IAM passa le operazioni dello stack a un ruolo di CloudFormation servizio, CloudFormation utilizza il ruolo di servizio per eseguire le operazioni di stack e fornire le risorse nel modello. CloudFormation Questo ruolo CloudFormation di servizio deve essere definito con le autorizzazioni per fornire il servizio per Servizi AWS conto del principale IAM. Questo approccio evita di concedere autorizzazioni dirette al responsabile IAM per fornire le AWS risorse definite nei modelli. CloudFormation Il principale IAM necessita delle autorizzazioni per la creazione CloudFormation dello stack e CloudFormation utilizza la policy del ruolo di servizio per effettuare chiamate anziché la policy del principale IAM.

Utilizzando l'approccio del ruolo di servizio e il principio del privilegio minimo, è possibile standardizzare il provisioning delle risorse nel proprio AWS ambiente e richiedere che gli utenti forniscano le risorse tramite IaC. CloudFormation Poiché le policy allegate ai principi IAM non contengono le autorizzazioni per il provisioning diretto delle AWS risorse, gli utenti devono utilizzarle per il provisioning delle stesse. CloudFormation

Questo capitolo esamina i seguenti meccanismi per la configurazione e la gestione dell'accesso al CloudFormation servizio e agli stack: CloudFormation

- Politiche basate sull'identità per CloudFormation— Utilizza questo tipo di policy per configurare a quali presidi IAM possono accedere CloudFormation e in quali azioni possono eseguire. CloudFormation
- Ruoli di servizio per CloudFormation— Crea un ruolo di servizio che CloudFormation consenta di creare, aggiornare o eliminare le risorse dello stack per conto del responsabile IAM che distribuisce lo stack. Il ruolo di servizio viene creato in IAM e può essere associato a uno o più stack.
- CloudFormation politiche dello stack— Utilizzate questo tipo di policy per determinare quando uno stack può essere aggiornato. Questo tipo di policy può aiutare a impedire che le risorse dello stack vengano aggiornate o eliminate involontariamente. Le policy dello stack vengono create e associate agli stack in. CloudFormation

Politiche basate sull'identità per CloudFormation

Considera i tipi di utenti a cui devono accedere AWS CloudFormation e considera le azioni in cui tali utenti devono eseguire. CloudFormation Le autorizzazioni utente vengono configurate tramite policy basate sull'identità, che vengono associate a un principale AWS Identity and Access Management (IAM), ad esempio un ruolo o un utente.

Quando si configura una policy basata sull'identità, sono necessari gli `Effect` elementi e. `Action` `Resource` Facoltativamente, puoi anche definire un elemento. `Condition` Per ulteriori informazioni su questi elementi, consulta il riferimento agli elementi della policy IAM JSON.

Questa sezione contiene i seguenti argomenti:

- Le migliori pratiche per la configurazione di policy basate sull'identità per l'accesso con privilegi minimi CloudFormation
- Esempi di politiche basate sull'identità per CloudFormation

Le migliori pratiche per la configurazione di policy basate sull'identità per l'accesso con privilegi minimi CloudFormation

- Per i responsabili IAM che richiedono autorizzazioni per accedere CloudFormation, è necessario bilanciare la necessità delle autorizzazioni per operare con il principio del privilegio minimo.

CloudFormation Per aiutarti a rispettare il principio del privilegio minimo, ti consigliamo di definire il principale IAM in base all'identità con azioni specifiche che consentano al principale di fare quanto segue:

- Crea, aggiorna ed elimina uno stack. CloudFormation
- Assegna uno o più ruoli di servizio con le autorizzazioni necessarie per distribuire le risorse definite nei modelli. CloudFormation Ciò consente di CloudFormation assumere il ruolo di servizio e fornire le risorse dello stack per conto del responsabile IAM.

- L'escalation dei privilegi si riferisce alla capacità di un utente con accesso di elevare i propri livelli di autorizzazione e compromettere la sicurezza. Il privilegio minimo è una best practice importante che può aiutare a prevenire l'escalation dei privilegi. Poiché CloudFormation supporta il provisioning di tipi di risorse IAM, come policy e ruoli, un responsabile IAM potrebbe aumentare i propri privilegi attraverso: CloudFormation
  - Utilizzo di uno CloudFormation stack per fornire a un principale IAM autorizzazioni, policy o credenziali altamente privilegiate: per evitare che ciò accada, consigliamo di utilizzare barriere di autorizzazione per limitare il livello di accesso per i principali IAM. I guardrail di autorizzazione impostano le autorizzazioni massime che una policy basata sull'identità può concedere a un responsabile IAM. Questo aiuta a prevenire l'escalation intenzionale e involontaria dei privilegi. È possibile utilizzare i seguenti tipi di politiche come protezioni per le autorizzazioni:
    - I limiti delle autorizzazioni definiscono le autorizzazioni massime che una policy basata sull'identità può concedere a un preside IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM.
    - In AWS Organizations, puoi utilizzare le policy di controllo del servizio (SCPs) per definire le autorizzazioni massime disponibili a livello organizzativo. SCPs riguardano solo i ruoli e gli utenti IAM gestiti dagli account dell'organizzazione. Puoi collegarti SCPs agli account, alle unità organizzative o alla radice dell'organizzazione. Per ulteriori informazioni, consulta Effetti delle SCP sulle autorizzazioni.
  - Creazione di un ruolo di CloudFormation servizio che offra autorizzazioni estese: per evitare che ciò accada, ti consigliamo di aggiungere le seguenti autorizzazioni granulari alle politiche basate sull'identità per i dirigenti IAM che utilizzeranno: CloudFormation
    - Utilizza la chiave `cloudformation:RoleARN` condition per controllare quali ruoli di servizio può utilizzare il preside IAM. CloudFormation
    - Consenti l'`iam:PassRole`azione solo per i ruoli CloudFormation di servizio specifici che il principale IAM deve passare.

Per ulteriori informazioni sul tagging, consulta Concessione a un IAM delle autorizzazioni principali per l'utilizzo di un CloudFormation ruolo di servizioin questa guida.

- Limita le autorizzazioni utilizzando barriere di autorizzazione, come i limiti delle autorizzazioni e SCPs, e concedi le autorizzazioni utilizzando una politica basata sull'identità o sulle risorse.

Esempi di politiche basate sull'identità per CloudFormation

Questa sezione contiene esempi di politiche basate sull'identità che dimostrano come concedere e negare le autorizzazioni per. CloudFormation È possibile utilizzare queste politiche di esempio per iniziare a progettare politiche personalizzate che aderiscano al principio del privilegio minimo.

Per un elenco di azioni e condizioni CloudFormation specifiche, consulta Azioni, risorse e chiavi di condizione per AWS CloudFormation e AWS CloudFormation condizioni. Per un elenco dei tipi di risorse da utilizzare con le condizioni, consulta il riferimento ai tipi di AWS risorse e proprietà.

Questa sezione contiene i seguenti esempi di politiche:

- Consenti l'accesso alla visualizzazione
- Consenti la creazione di stack in base al modello
- Negare l'aggiornamento o l'eliminazione di uno stack

Consenti l'accesso alla visualizzazione

L'accesso alla visualizzazione è il tipo di accesso meno privilegiato a. CloudFormation Questo tipo di policy potrebbe essere appropriato per i dirigenti IAM che desiderano visualizzare tutti gli stack di. CloudFormation Account AWS La seguente policy di esempio concede le autorizzazioni per visualizzare i dettagli di qualsiasi CloudFormation stack dell'account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStackResource",
```

```
        "cloudformation:DescribeStackResources"
      ],
      "Resource": "*"
    }
  ]
}
```

Consenti la creazione di stack in base al modello

La seguente policy di esempio consente ai responsabili IAM di creare stack utilizzando solo i CloudFormation modelli archiviati in uno specifico bucket Amazon Simple Storage Service (Amazon S3). Il nome del bucket è. `my-CFN-templates` Puoi caricare modelli approvati in questo bucket. La chiave di `cloudformation:TemplateUrl` condizione nella policy impedisce al responsabile IAM di utilizzare altri modelli per creare stack.

> **Important**
>
> Consenti al principale IAM di avere accesso in sola lettura a questo bucket S3. Questo aiuta a impedire al responsabile IAM di aggiungere, rimuovere o modificare i modelli approvati.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:TemplateUrl": "https:// my-CFN-templates.s3.amazonaws.com/*"
        }
      }
    }
  ]
}
```

Negare l'aggiornamento o l'eliminazione di uno stack

Per proteggere CloudFormation stack specifici che forniscono AWS risorse aziendali critiche, puoi limitare le azioni di aggiornamento ed eliminazione per quello stack specifico. Puoi consentire queste azioni solo per alcuni principi IAM specificati e negarle per qualsiasi altro principale IAM nell'ambiente. La seguente dichiarazione politica nega le autorizzazioni per aggiornare o eliminare uno CloudFormation stack specifico in uno specifico and. Regione AWS Account AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>"
    }
  ]
}
```

Questa dichiarazione politica nega le autorizzazioni per aggiornare o eliminare lo `MyProductionStack` CloudFormation stack, che si trova in e in. `us-east-1` Regione AWS `123456789012` Account AWSÈ possibile visualizzare l'ID dello stack nella console. CloudFormation Di seguito sono riportati alcuni esempi di come è possibile modificare l'`Resource`elemento di questa dichiarazione in base al proprio caso d'uso:

- È possibile aggiungere più CloudFormation stack IDs nell'`Resource`elemento di questa politica.
- Puoi utilizzarlo `arn:aws:cloudformation:us-east-1:123456789012:stack/*` per impedire ai responsabili IAM di aggiornare o eliminare qualsiasi stack presente nell'account `us-east-1` Regione AWS e nell'account. `123456789012`

Un passo importante è decidere quale policy deve contenere questa dichiarazione. È possibile aggiungere questa dichiarazione alle seguenti politiche:

- La policy basata sull'identità associata al principio IAM: l'inserimento della dichiarazione in questa policy impedisce al principale IAM specifico di creare o eliminare uno stack specifico. CloudFormation
- Un limite di autorizzazioni collegato al principio IAM: l'inserimento della dichiarazione in questa policy crea una barriera di autorizzazioni. Impedisce a più di un principale IAM di creare o eliminare uno CloudFormation stack specifico, ma non limita tutti i principali dell'ambiente.
- Un SCP collegato a un account, unità organizzativa o organizzazione: l'inserimento della dichiarazione in questa politica crea un limite di autorizzazioni. Impedisce a tutti i responsabili IAM dell'account, dell'unità organizzativa o dell'organizzazione di destinazione di creare o eliminare uno stack specifico. CloudFormation

  Tuttavia, se non consenti ad almeno un principale IAM, un principale privilegiato, di aggiornare o eliminare lo CloudFormation stack, non sarai in grado di apportare alcuna modifica, se necessario, alle risorse fornite tramite questo stack. Un utente o una pipeline di sviluppo (consigliato) può assumere questo principio privilegiato. Se desideri implementare la restrizione come SCP, ti consigliamo invece la seguente dichiarazione politica.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:123456789012:stack/
MyProductionStack/<stack_ID>",
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN": [
            "<ARN of the allowed privilege IAM principal>"
          ]
        }
      }
    }
  ]
}
```

In questa dichiarazione, l'`Condition`elemento definisce il principio IAM escluso da SCP. Questa istruzione nega qualsiasi autorizzazione principale IAM per aggiornare o eliminare gli CloudFormation stack a meno che l'ARN del principale IAM non corrisponda all'ARN nell'elemento. `Condition` La chiave di `aws:PrincipalARN` condizione accetta un elenco, il che significa che puoi escludere più di un principale IAM dalle restrizioni, in base alle esigenze del tuo ambiente. Per un SCP simile che impedisce modifiche alle CloudFormation risorse, vedi SCP-CLOUDFORMATION-1 (). GitHub

Ruoli di servizio per CloudFormation

Un ruolo di servizio è un ruolo AWS Identity and Access Management (IAM) che consente di AWS CloudFormation creare, aggiornare o eliminare risorse dello stack. Se non fornisci un ruolo di servizio, CloudFormation utilizza le credenziali del principale IAM per eseguire le operazioni dello stack. Se crei un ruolo di servizio CloudFormation e lo specifichi durante la creazione dello stack, CloudFormation utilizza le credenziali del ruolo di servizio per eseguire le operazioni, anziché le credenziali del principale IAM.

Quando si utilizza un ruolo di servizio, la policy basata sull'identità associata al principale IAM non richiede autorizzazioni per fornire tutte le risorse definite nel modello. AWS CloudFormation Se non siete pronti a fornire AWS risorse per operazioni aziendali critiche attraverso una pipeline di sviluppo (una best practice AWS consigliata), l'utilizzo di un ruolo di servizio può aggiungere un ulteriore livello di protezione per la gestione delle risorse. AWS I vantaggi di questo approccio sono:

- I responsabili IAM dell'organizzazione seguono un modello con privilegi minimi che impedisce loro di creare o modificare AWS manualmente le risorse nell'ambiente.
- Per creare, aggiornare o eliminare le AWS risorse, i dirigenti IAM devono utilizzare. CloudFormation Ciò standardizza l'approvvigionamento delle risorse tramite l'infrastruttura come codice.

Ad esempio, per creare uno stack che contenga un'istanza Amazon Elastic Compute Cloud (Amazon EC2), il responsabile IAM deve disporre delle autorizzazioni per creare istanze EC2 tramite la propria policy basata sull'identità. CloudFormation Può invece assumere un ruolo di servizio che dispone delle autorizzazioni per creare istanze EC2 per conto del principale. Con questo approccio, il responsabile IAM può creare lo stack e non è necessario concedere al responsabile IAM autorizzazioni troppo ampie per un servizio a cui non dovrebbe avere accesso regolare.

Per utilizzare un ruolo di servizio per creare CloudFormation stack, i responsabili IAM devono disporre delle autorizzazioni a cui trasferire il ruolo di servizio e la politica di fiducia del ruolo di servizio deve consentire di assumere il ruolo. CloudFormation CloudFormation

Questa sezione contiene i seguenti argomenti:

- Implementazione del privilegio minimo per i ruoli di servizio CloudFormation
- Configurazione dei ruoli di servizio
- Concessione a un IAM delle autorizzazioni principali per l'utilizzo di un CloudFormation ruolo di servizio
- Configurazione di una politica di fiducia per il ruolo di servizio CloudFormation
- Associazione di un ruolo di servizio a uno stack

Implementazione del privilegio minimo per i ruoli di servizio CloudFormation

In un ruolo di servizio, si definisce una politica di autorizzazioni che specifica esplicitamente quali azioni il servizio può eseguire. Queste potrebbero non essere le stesse azioni che un preside IAM può eseguire. Ti consigliamo di utilizzare i CloudFormation modelli a ritroso per creare un ruolo di servizio che aderisca al principio del privilegio minimo.

Definire correttamente l'ambito della policy basata sull'identità di un principale IAM in modo da assegnare solo ruoli di servizio specifici e definire la policy di fiducia di un ruolo di servizio in modo da consentire solo a soggetti specifici di assumere il ruolo aiuta a prevenire il possibile aumento dei privilegi attraverso i ruoli di servizio.

Configurazione dei ruoli di servizio

> **Note**
>
> I ruoli di servizio sono configurati in IAM. Per creare un ruolo di servizio, è necessario disporre delle autorizzazioni necessarie. Un preside IAM con le autorizzazioni per creare un ruolo e allegare qualsiasi policy può aumentare le proprie autorizzazioni. AWS consiglia di creare un ruolo di servizio per ciascuno Servizio AWS per ogni caso d'uso. Dopo aver creato i ruoli di CloudFormation servizio per i tuoi casi d'uso, puoi consentire agli utenti di passare solo il ruolo di servizio approvato a CloudFormation. Per esempi di policy basate sull'identità che consentono agli utenti di creare ruoli di servizio, consulta le autorizzazioni dei ruoli di servizio nella documentazione IAM.

Per istruzioni su come creare ruoli di servizio, consulta Creazione di un ruolo per delegare le autorizzazioni a un. Servizio AWS Specifica CloudFormation (`cloudformation.amazonaws.com`) come servizio che può assumere il ruolo. Ciò impedisce a un responsabile IAM di assumere autonomamente il ruolo o di passarlo ad altri servizi. Quando si configura un ruolo di servizio, sono necessari `Resource` gli elementi`Action`, e. `Effect` Facoltativamente, puoi anche definire un `Condition` elemento.

Per ulteriori informazioni su questi elementi, consulta il riferimento agli elementi della policy IAM JSON. Per un elenco completo di azioni, risorse e chiavi di condizione, consulta Azioni, risorse e chiavi di condizione per la gestione delle identità e degli accessi.

Concessione a un IAM delle autorizzazioni principali per l'utilizzo di un CloudFormation ruolo di servizio

Per fornire risorse CloudFormation utilizzando il ruolo di CloudFormation servizio, il responsabile IAM deve disporre delle autorizzazioni per passare il ruolo di servizio. Puoi limitare le autorizzazioni del principale IAM a passare solo determinati ruoli specificando l'ARN del ruolo nelle autorizzazioni del principale. Per ulteriori informazioni, consulta Concessione a un utente delle autorizzazioni per passare un ruolo a un utente nella documentazione IAM. Servizio AWS

La seguente dichiarazione politica basata sull'identità IAM consente al principale di assegnare i ruoli, inclusi i ruoli di servizio, che si trovano nel percorso. `cfnroles` Il principale non può assegnare ruoli che si trovano in un percorso diverso.

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/cfnroles/*"
}
```

Un altro approccio per limitare i principali a determinati ruoli consiste nell'utilizzare un prefisso per i nomi dei ruoli di CloudFormation servizio. La seguente dichiarazione politica consente ai presidi IAM di passare solo i ruoli con un prefisso. `CFN-`

```
{
"Sid": "AllowPassingAppRoles",
"Effect": "Allow",
```

```
"Action": "iam:PassRole",
"Resource": "arn:aws:iam::<account ID>:role/CFN-*"
}
```

Oltre alle precedenti dichiarazioni politiche, puoi utilizzare la chiave `cloudformation:RoleARN` condition per fornire ulteriori controlli granulari nella politica basata sull'identità, per un accesso con privilegi minimi. La seguente dichiarazione politica consente al responsabile IAM di creare, aggiornare ed eliminare gli stack solo se ricoprono un ruolo di servizio specifico. CloudFormation Come variante, è possibile definire più ARNs di un ruolo di CloudFormation servizio nella chiave di condizione.

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringEquals": {
      "cloudformation:RoleArn": [
        "<ARN of the specific CloudFormation service role>"
      ]
    }
  }
}
```

Inoltre, puoi anche utilizzare la chiave di `cloudformation:RoleARN` condizione per impedire a un principale IAM di passare un ruolo di CloudFormation servizio altamente privilegiato per le operazioni di stack. L'unica modifica richiesta è nell'operatore condizionale, da a. `StringEquals` `StringNotEquals`

```
{
  "Sid": "RestrictCloudFormationAccess",
  "Effect": "Allow",
  "Action": [
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:UpdateStack"
```

```
  ],
  "Resource": "arn:aws:iam::<account ID>:role/CFN-*",
  "Condition": {
    "StringNotEquals": {
      "cloudformation:RoleArn": [
        "<ARN of a privilege CloudFormation service role>"
      ]
    }
  }
}
```

Configurazione di una politica di fiducia per il ruolo di servizio CloudFormation

Una policy di trust per i ruoli è una policy necessaria basata sulle risorse associata a un ruolo IAM. Una policy di fiducia definisce quali dirigenti IAM possono assumere il ruolo. In una politica di fiducia, puoi specificare utenti, ruoli, account o servizi come responsabili. Per impedire ai responsabili IAM di trasferire i ruoli di servizio CloudFormation ad altri servizi, puoi specificare CloudFormation come principale la politica di fiducia del ruolo.

La seguente politica di fiducia consente solo al CloudFormation servizio di assumere il ruolo di servizio.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {
      "Service": "cloudformation.amazonaws.com"
    },
    "Action": "sts:AssumeRole"
  }
}
```

Associazione di un ruolo di servizio a uno stack

Dopo aver creato un ruolo di servizio, è possibile associarlo a uno stack al momento della creazione dello stack. Per ulteriori informazioni, consulta Configurare le opzioni dello stack. Prima di specificare un ruolo di servizio, assicurati che i responsabili IAM dispongano delle autorizzazioni per passarlo.

Per ulteriori informazioni, consulta Concessione a un IAM delle autorizzazioni principali per l'utilizzo di un CloudFormation ruolo di servizio.

CloudFormation politiche dello stack

Le policy dello stack possono aiutare a impedire che le risorse dello stack vengano aggiornate o eliminate involontariamente durante un aggiornamento dello stack. Una politica dello stack è un documento JSON che definisce le azioni di aggiornamento che possono essere eseguite su risorse designate. Per impostazione predefinita, qualsiasi principale IAM con `cloudformation:UpdateStack` autorizzazioni può aggiornare tutte le risorse di uno stack. AWS CloudFormation Gli aggiornamenti possono causare interruzioni oppure eliminare e sostituire completamente le risorse. È possibile utilizzare una politica di stack per configurare le autorizzazioni con privilegi minimi. Le policy dello stack possono fornire un ulteriore livello di protezione.

Per impostazione predefinita, una policy di stack aiuta a proteggere tutte le risorse dello stack. Tuttavia, il vantaggio principale delle policy di stack è che forniscono un controllo granulare per ogni AWS risorsa distribuita in uno stack. CloudFormation È possibile utilizzare una policy di stack per proteggere solo risorse specifiche in uno stack e consentire l'aggiornamento o l'eliminazione di altre risorse nello stesso stack. Per consentire gli aggiornamenti per risorse specifiche, includi una `Allow` dichiarazione esplicita per tali risorse nella tua politica dello stack.

Le policy di stack forniscono controlli preventivi per gli CloudFormation stack a cui sono collegate. Ogni stack può avere una sola policy di stack, ma è possibile utilizzare tale policy per proteggere tutte le risorse all'interno di quello stack. È possibile applicare una politica di stack a più stack.

Ad esempio, immagina di avere una pipeline che produce artefatti sensibili e li archivia temporaneamente in un bucket Amazon Simple Storage Service (Amazon S3) per un'ulteriore elaborazione. Il bucket S3 viene fornito da e tutti i controlli di sicurezza CloudFormation necessari sono stati implementati. Senza politiche di stack, uno sviluppatore potrebbe modificare intenzionalmente o meno la destinazione degli artefatti della pipeline in un bucket S3 meno sicuro ed esporre dati sensibili. Se allo stack viene applicata una policy di stack, questa impedisce agli utenti autorizzati di eseguire azioni di aggiornamento o eliminazione indesiderate.

Questa sezione contiene i seguenti argomenti:

- Configurazione delle politiche dello stack
- Impostazione e sovrascrittura delle politiche di stack
- Limitazione e richiesta di politiche di stack

Configurazione delle politiche dello stack

Quando configuri una policy di stack, sono necessari gli elementi, `Effect`Action, `Principal` e. `Resource` Facoltativamente, puoi anche definire un `Condition` elemento.

Quando si crea una politica dello stack, per impostazione predefinita, impedisce gli aggiornamenti per tutte le risorse dello stack. È possibile personalizzare la politica dello stack per definire quali azioni sono esplicitamente consentite. Se si desidera invertire la politica, è possibile definire un'`Allow`istruzione che consenta tutte le azioni e quindi specificare `Deny` istruzioni esplicite che impediscano azioni solo su risorse specifiche. Per riferimento, consultate questo esempio di stack policy nella documentazione. CloudFormation

Per ulteriori informazioni sull'utilizzo di questi elementi per creare policy di stack personalizzate e altri esempi di policy, consulta Definizione di una politica di stack e Altri esempi di politiche di stack nella documentazione. CloudFormation

Impostazione e sovrascrittura delle politiche di stack

Dopo aver creato una policy di stack, la associ a uno stack. Se state assegnando la politica dello stack a uno stack esistente, dovete usare il (). AWS Command Line Interface AWS CLI Tuttavia, se state assegnando la policy al momento della creazione dello stack, potete utilizzare la console o il. CloudFormation AWS CLI Per istruzioni, consulta Impostazione di una politica dello stack nella documentazione. CloudFormation

Se desideri consentire agli utenti di aggiornare o eliminare le risorse nello stack, devi sostituire temporaneamente la politica dello stack. Questo override consente di eseguire azioni altrimenti negate sulle risorse protette in quello stack. Per istruzioni, consulta Aggiornamento delle risorse protette nella CloudFormation documentazione.

Limitazione e richiesta di politiche di stack

Come best practice per le autorizzazioni con privilegi minimi, prendi in considerazione la possibilità di richiedere ai principali IAM di assegnare policy di stack e di limitare le policy di stack che i principali IAM possono assegnare. Molti dirigenti IAM non dovrebbero avere i permessi per creare e assegnare policy di stack personalizzate ai propri stack.

Dopo aver creato le policy degli stack, ti consigliamo di caricarle in un bucket S3. Puoi quindi fare riferimento a queste politiche di stack utilizzando la chiave `cloudformation:StackPolicyUrl` condition e fornendo l'URL della politica di stack nel bucket S3.

Concessione delle autorizzazioni per allegare le politiche dello stack

Come best practice per le autorizzazioni con privilegi minimi, prendi in considerazione la possibilità di limitare le policy dello stack che i responsabili IAM possono allegare agli stack. CloudFormation Nella policy basata sull'identità per il principale IAM, puoi specificare quali policy dello stack il preside IAM ha le autorizzazioni da assegnare. Ciò impedisce al principale IAM di allegare qualsiasi policy di stack, il che può ridurre il rischio di errori di configurazione.

Ad esempio, un'organizzazione potrebbe avere team diversi con requisiti diversi. Di conseguenza, ogni team crea politiche di stack per gli stack specifici del team CloudFormation . In un ambiente condiviso, se tutti i team archiviano le proprie politiche di stack nello stesso bucket S3, un membro del team potrebbe allegare una policy di stack disponibile ma non destinata agli stack del proprio team. CloudFormation Per evitare questo scenario, puoi definire una dichiarazione di policy che consenta ai responsabili IAM di allegare solo policy di stack specifiche.

La seguente policy di esempio consente al principale IAM di allegare policy di stack archiviate in una cartella specifica del team in un bucket S3. È possibile archiviare le politiche di stack approvate in questo bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:SetStackPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "cloudformation:StackPolicyUrl": "<Bucket URL>/<Team folder>/*"
        }
      }
    }
  ]
}
```

Questa dichiarazione politica non richiede che un preside IAM assegni una policy di stack a ogni stack. Anche se il responsabile IAM dispone delle autorizzazioni per creare stack con una policy di stack specifica, può scegliere di creare uno stack che non dispone di una policy di stack.

Richiedere politiche di stack

Per garantire che tutti i responsabili IAM assegnino policy di stack ai propri stack, puoi definire una policy di controllo del servizio (SCP) o un limite di autorizzazioni come barriera preventiva.

La seguente policy di esempio mostra come configurare un SCP che richiede ai dirigenti IAM di assegnare una policy di stack durante la creazione di uno stack. Se il principale IAM non allega una policy di stack, non può creare lo stack. Inoltre, questa policy impedisce ai responsabili IAM con autorizzazioni di aggiornamento dello stack di rimuovere la policy dello stack durante un aggiornamento. La policy limita l'azione utilizzando la chiave condition. `cloudformation:UpdateStack` `cloudformation:StackPolicyUrl`

```
        {
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "cloudformation:StackPolicyUrl": "true"
        }
      }
    }
  ]
}
```

Includendo questa dichiarazione politica in un SCP anziché in un limite di autorizzazioni, puoi applicare il tuo guardrail a tutti gli account dell'organizzazione. Questo può fare quanto segue:

1. Riduci lo sforzo di collegare la policy individualmente a più principi IAM in un Account AWS unico. I limiti delle autorizzazioni possono essere collegati direttamente solo a un principale IAM.
2. Riduci lo sforzo di creare e gestire più copie del limite delle autorizzazioni per diversi utenti. Account AWS Ciò riduce il rischio di errori di configurazione in più limiti di autorizzazioni identici.

> **Note**
>
> SCPs e i limiti delle autorizzazioni sono barriere di autorizzazione che definiscono le autorizzazioni massime disponibili per i responsabili IAM in un account o in un'organizzazione. Queste politiche non concedono autorizzazioni ai presidi IAM. Se desideri standardizzare il requisito che tutti i responsabili IAM del tuo account o della tua organizzazione assegnino policy di stack, devi utilizzare sia le barriere di autorizzazione che le politiche basate sull'identità.

Configurazione delle autorizzazioni con privilegi minimi per le risorse fornite tramite CloudFormation

AWS CloudFormation consente di fornire molti tipi diversi di AWS risorse. Le risorse assegnate richiedono un proprio set di autorizzazioni per funzionare come previsto e per configurare chi ha accesso a tali risorse. Nel capitolo precedente sono state esaminate le opzioni per la configurazione delle autorizzazioni di accesso e utilizzo del servizio. CloudFormation Questo capitolo illustra come applicare il principio del privilegio minimo alle risorse fornite tramite. CloudFormation

In questa guida, sarebbe praticamente impossibile esaminare le raccomandazioni e le migliori pratiche di sicurezza per ogni tipo di AWS risorsa tramite cui è possibile effettuare il provisioning. CloudFormation In caso di domande relative a un servizio specifico, si consiglia di consultare la documentazione relativa a tale servizio. La maggior parte dei Servizio AWS documenti contiene una sezione sulla sicurezza e informazioni sulle autorizzazioni necessarie per utilizzare quel servizio. Per un elenco completo della Servizio AWS documentazione, vedere AWS Documentazione.

Di seguito sono riportati i passaggi di alto livello, indipendenti dal servizio, che è possibile eseguire per creare CloudFormation modelli che rispettino il principio del privilegio minimo:

1. Prepara un elenco di risorse che intendi utilizzare per il provisioning. CloudFormation
2. Consulta la AWS documentazione per i servizi corrispondenti e consulta le sezioni sulla sicurezza e la gestione degli accessi. Questo ti aiuta a comprendere i requisiti e i consigli specifici del servizio.
3. Utilizza le informazioni raccolte nei passaggi precedenti per progettare CloudFormation modelli e politiche associate che consentano solo le autorizzazioni richieste e neghino tutte le altre.

Successivamente, questa guida esamina un esempio di come applicare il principio del privilegio minimo nei CloudFormation modelli, utilizzando un caso d'uso reale.

Esempio: bucket Amazon S3 per l'archiviazione degli artefatti della pipeline

Questo esempio crea un bucket Amazon Simple Storage Service (Amazon S3) che viene utilizzato per archiviare gli artefatti del progetto. AWS CodeBuild AWS CodePipelineutilizza questi artefatti

memorizzati. Puoi consentire CodeBuild e accedere CodePipeline a questo bucket S3 tramite i ruoli di servizio e controllare tale accesso utilizzando una policy sui bucket di Amazon S3. Di seguito sono riportati i nomi delle risorse utilizzati in questo esempio:

- `Deployfiles_build`è il nome del CodeBuild progetto.
- `Deployment-Pipeline`è il nome della pipeline in CodePipeline.

Definisci il bucket Amazon S3

Innanzitutto, definisci il bucket S3 nel CloudFormation modello, che è un file di testo in formato YAML.

```
amzn-s3-demo-bucket:
  Type: AWS::S3::Bucket
  Properties:
    PublicAccessBlockConfiguration:
        BlockPublicAcls: true
        BlockPublicPolicy: true
        IgnorePublicAcls: true
        RestrictPublicBuckets: true
```

Definizione della policy sui bucket di Amazon S3

Successivamente, nel CloudFormation modello, crei una bucket policy che consenta solo al `Deployfiles_build` progetto e alla `Deployment-Pipeline` pipeline di accedere al bucket.

```
MyBucketPolicy:
  Type: AWS::S3::BucketPolicy
  Properties:
    Bucket: !Ref amzn-s3-demo-bucket
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
      - Sid: "S3ArtifactRepoAccess"
        Effect: Allow
        Action:
          - ‘s3:GetObject'
          - ‘s3:GetObjectVersion'
          - ‘s3:PutObject'
          - ‘s3:GetBucketVersioning'
        Resource:
```

```
          - !Sub 'arn:aws:s3:::${amzn-s3-demo-bucket}'
          - !Sub 'arn:aws:s3:::${amzn-s3-demo-bucket}/*'
        Principal:
          Service:
            - codebuild.amazonaws.com
            - codepipeline.amazonaws.com
        Condition:
          StringLike:
            'aws:SourceArn':
              - !Sub 'arn:aws:codebuild:${AWS::Region}:${AWS::AccountId}:project/
Deployfiles_build'
              - !Sub 'arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline'
              - !Sub 'arn:aws:codepipeline:${AWS::Region}:${AWS::AccountId}:Deployment-
Pipeline/*'
```

Tieni presente quanto segue su questa policy sui bucket:

- L'`Resource`elemento elenca due diversi tipi di risorse che utilizzano i seguenti formati Amazon Resource Name (ARN):
  - Il formato ARN di un oggetto S3 è. `arn:$`*`<Partition>`*`:s3:::$`*`<BucketName>`*`/$`*`<ObjectName>`*
  - Il formato ARN di un bucket S3 è. `arn:$`*`<Partition>`*`:s3:::$`*`<BucketName>`*

  `s3:GetObjects3:GetObjectVersion`, e `s3:PutObject` richiedono un tipo di risorsa oggetto S3 e `s3:GetBucketVersioning` richiedono un tipo di risorsa bucket S3. Per ulteriori informazioni sui tipi di risorse richiesti per ogni azione, consulta Azioni, risorse e chiavi di condizione per Amazon S3.
- L'`Principal`elemento elenca le entità autorizzate a eseguire le azioni di Amazon S3 definite nell'istruzione. In questo caso, solo CodeBuild e CodePipeline sono autorizzati a eseguire queste azioni.
- L'`Condition`elemento limita ulteriormente l'accesso al bucket S3 in modo che solo il `Deployfiles_build` CodeBuild progetto, la pipeline e le azioni della `Deployment-Pipeline` CodePipeline pipeline possano accedere al bucket.

Crea i ruoli di servizio

Sebbene la policy del bucket controlli l'accesso al bucket, non concede autorizzazioni CodeBuild e CodePipeline per accedervi. Per concedere l'accesso, è necessario creare un ruolo di servizio per

ogni servizio e aggiungere la seguente dichiarazione a ciascuno di essi. I ruoli dei servizi CodeBuild e CodePipeline consentono ai servizi di accedere al bucket S3 e ai suoi oggetti.

```
Sid: "ViewAccessToS3ArtifactRepo"
Effect: Allow
Action:
  - ‘s3:GetObject'
  - ‘s3:GetObjectVersion'
  - ‘s3:PutObject'
  - ‘s3:GetBucketVersioning'
Resource:
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}'
  - !Sub ‘arn:aws:s3:::${BuildArtifactsBucket}/*'
```

Procedure consigliate per le autorizzazioni con privilegi minimi per AWS CloudFormation

Questa guida esamina diversi approcci e alcuni tipi di politiche che è possibile utilizzare per configurare l'accesso con privilegi minimi e il relativo approvvigionamento delle risorse. AWS CloudFormation CloudFormation Questa guida si concentra sulla configurazione dell'accesso CloudFormation tramite i principi IAM, i ruoli di servizio e le policy di stack. I consigli e le best practice inclusi sono progettati per proteggere gli account e lo stack di risorse da azioni indesiderate da parte di utenti autorizzati e da malintenzionati che potrebbero sfruttare autorizzazioni eccessive.

Di seguito è riportato un riepilogo delle best practice illustrate in questa guida. Queste best practice possono aiutarti a rispettare il principio del privilegio minimo durante la configurazione delle autorizzazioni d'uso CloudFormation e del provisioning delle risorse tramite: CloudFormation

- Determina il livello di accesso necessario agli utenti e ai team per utilizzare il CloudFormation servizio e concedi solo l'accesso minimo richiesto. Ad esempio, concedi l'accesso alla visualizzazione a stagisti e revisori e non consenti a questi tipi di utenti di creare, aggiornare o eliminare gli stack.
- Per i responsabili IAM che devono fornire più tipi di AWS risorse tramite CloudFormation stack, è consigliabile utilizzare i ruoli di servizio per consentire l'erogazione delle risorse CloudFormation per conto del committente, anziché configurare l'accesso Servizi AWS a quelle previste dalle politiche basate sull'identità del committente.
- Nelle politiche basate sull'identità per i presidi IAM, utilizza la chiave `cloudformation:RoleARN` condition per controllare quali ruoli di servizio possono essere passati. CloudFormation
- Per evitare l'escalation dei privilegi, procedi come segue:
  - Monitora rigorosamente tutti i principali IAM che hanno accesso al CloudFormation servizio e i livelli di accesso di cui dispongono.
  - Monitora rigorosamente quali utenti possono accedere a questi principi IAM.
  - Monitora l'attività dei responsabili IAM a cui è possibile assegnare un ruolo di servizio privilegiato. CloudFormation Anche se potrebbero non disporre delle autorizzazioni necessarie per creare risorse IAM tramite la loro policy basata sull'identità, il ruolo di servizio che possono assegnare potrebbe creare risorse IAM.

- Specifica una policy di stack ogni volta che crei uno stack con risorse critiche. Questo può aiutare a proteggere le risorse critiche dello stack da aggiornamenti involontari che potrebbero causare l'interruzione o la sostituzione di tali risorse.
- Per le risorse fornite tramite CloudFormation, consulta i consigli sulla gestione degli accessi e le migliori pratiche di sicurezza per quel servizio.
- Per completare i consigli di questa guida per le politiche basate sull'identità e le politiche basate sulle risorse, prendi in considerazione l'implementazione di controlli di sicurezza aggiuntivi per le autorizzazioni con privilegi minimi, come le politiche di controllo del servizio () e i limiti delle autorizzazioni. SCPs Per ulteriori informazioni, consulta Fasi successive.

La CloudFormation documentazione contiene ulteriori best practice e best practice di sicurezza che possono aiutarti a utilizzare in modo più efficace e sicuro. CloudFormation Inoltre, consulta Le migliori pratiche per la configurazione di policy basate sull'identità per l'accesso con privilegi minimi CloudFormation questa guida.

Fasi successive

È possibile utilizzare le informazioni e gli esempi contenuti in questa guida per iniziare ad applicare il principio del privilegio minimo nella propria organizzazione. Ti consigliamo di consultare le risorse aggiuntive contenute nella Resources sezione, che contiene documentazione, riferimenti e strumenti che possono aiutarti a perfezionare le tue politiche.

Questa guida ha lo scopo di aiutarti a iniziare a implementare l'accesso con privilegi minimi per. AWS CloudFormation Tuttavia, esistono altri tipi di policy che possono aiutarvi a rafforzare il principio del privilegio minimo nella vostra organizzazione. In base all'ambiente e ai requisiti aziendali, è possibile implementare controlli aggiuntivi non descritti in questa guida. Come passaggio successivo e per ulteriori informazioni, si consiglia di consultare i seguenti argomenti relativi ai privilegi minimi e alla configurazione dell'accesso e delle autorizzazioni:

- Limiti delle autorizzazioni per le entità IAM
- Politiche di controllo dei servizi (SCP)
- Ruoli per l'accesso su più account
- Federazione delle identità
- Visualizzazione delle informazioni relative all'ultimo accesso per IAM

I seguenti strumenti possono aiutarti a monitorare l'accesso e le autorizzazioni con privilegi minimi per: CloudFormation

- AWS Identity and Access Management Access Analyzer
- Puoi utilizzare la scheda Access Advisor nella console AWS Identity and Access Management (IAM) per identificare le autorizzazioni eccessive per le identità IAM. Per un esempio, consulta Rafforzare le autorizzazioni S3 per gli utenti e i ruoli IAM utilizzando la cronologia degli accessi alle azioni S3 (post del blog).AWS
- Puoi utilizzare uno strumento di linting, come cfn-policy-validator(GitHub), per identificare le autorizzazioni eccessive.

Se hai dimestichezza con la creazione e la gestione delle CloudFormation autorizzazioni, ti consigliamo di utilizzare pipeline di integrazione e distribuzione continua (CI/CD) per distribuire i tuoi modelli. CloudFormation Ciò riduce il rischio di errori umani e accelera il processo di implementazione.

Resources

AWS CloudFormation documentazione

- Controllo dell'accesso con AWS Identity and Access Management
- AWS riferimento ai tipi di risorse e proprietà
- Impostazione delle AWS CloudFormation opzioni dello stack
- AWS CloudFormation ruolo del servizio

AWS Identity and Access Management documentazione (IAM)

- Politiche e autorizzazioni in IAM
- Documentazione di riferimento degli elementi delle policy JSON IAM
- Logica di valutazione delle policy
- Servizi AWS che funzionano con IAM
- Creare un ruolo per delegare le autorizzazioni a un Servizio AWS
- Problema del "confused deputy"
- Best practice per la sicurezza in IAM

Altro AWS riferimenti

- Azioni, risorse e chiavi di condizione per Servizi AWS (Service Authorization Reference)
- Concedi l'accesso con il minimo privilegio (AWS Well-Architected Framework)
- Tecniche per scrivere politiche IAM con privilegi minimi (AWS post sul blog)

Cronologia dei documenti

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

Modifica	Descrizione	Data
Aggiornamenti significativi	Abbiamo rivisto e perfezionato in modo significativo le linee guida e le dichiarazioni politiche di esempio per affrontare i casi d'uso organizzativi comuni.	5 maggio 2023
Pubblicazione iniziale	—	9 marzo 2023

AWS Glossario delle linee guida prescrittive

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

Numeri

7 R

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

- Refactor/re-architect — Sposta un'applicazione e modificane l'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 Amazon PostgreSQL-Compatible Aurora.
- 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 su 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

A2A () Agent-to-Agent

Un protocollo statico per la collaborazione tra agenti che supporta la delega delle attività e il trasferimento dello stato.

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.

Agente

Un sistema di intelligenza artificiale in grado di ragionare, pianificare e intraprendere azioni in modo autonomo utilizzando strumenti per raggiungere gli obiettivi.

Agente Ops

Pratiche operative per la creazione, il test, l'implementazione e l'esecuzione di agenti di intelligenza artificiale in produzione su larga scala.

funzione aggregata

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

Intelligenza artificiale

Vedi intelligenza artificiale.

AIOps

Guarda le operazioni di intelligenza artificiale.

anonimizzazione

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

anti-modello

Una soluzione utilizzata 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 viene utilizzato AIOps nella strategia di migrazione AWS , 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 for 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 disturbare 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.

blue/green dispiegamento

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, consulta l'indicatore Implementare le procedure break-glass nella guida. AWS Well-Architected

strategia brownfield

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

cache del buffer

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

capacità di business

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

pianificazione della continuità operativa (BCP)

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

C

CAF

Vedi AWS Cloud Adoption Framework.

implementazione canaria

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

CoE

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.

Sviluppatore cittadino

Un utente aziendale che crea applicazioni di intelligenza artificiale utilizzando piattaforme senza code/low codice senza competenze tecniche specializzate.

crittografia lato client

Crittografia dei dati localmente, prima che il bersaglio li Servizio AWS riceva.

centro di eccellenza del cloud (CCoE)

Un team multidisciplinare che guida le iniziative di adozione del cloud in tutta l'organizzazione, tra cui lo sviluppo di best practice per il cloud, la mobilitazione delle risorse, la definizione delle tempistiche di migrazione e la guida dell'organizzazione attraverso trasformazioni su larga scala. Per ulteriori informazioni, consulta i post di CCoE 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 dimensionare l'adozione del cloud (ad esempio, creazione di una zona di destinazione, definizione di un CCoE, definizione di un modello operativo)
- Migrazione: migrazione di singole applicazioni
- Re-invention — Ottimizzazione di prodotti e servizi e innovazione nel cloud

Queste fasi sono state definite da Stephen Orban nel post del blog The Journey Toward Cloud-First & the Stages of Adoption sul blog Enterprise Strategy. Cloud AWS Per informazioni sulla loro relazione con la 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 CI/CD pipeline 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 continue () 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.

difesa in profondità

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 approccio di difesa approfondita potrebbe combinare autenticazione a più fattori, segmentazione della rete e 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 Workload su AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Vedi linguaggio di manipolazione del database.

progettazione basata sul dominio

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

DOTT.

Vedi disaster recovery.

rilevamento della deriva

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

DVSM

Vedi la mappatura del flusso di valore dello sviluppo.

E

EDA

Vedi analisi esplorativa dei dati.

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. Big-endian i sistemi memorizzano per primi il byte più importante. Little-endian i sistemi memorizzano per primi 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 con schema a stella. Memorizza dati quantitativi sulle operazioni aziendali. In genere, una tabella dei fatti contiene due tipi di colonne: quelle che contengono misure e quelle che contengono una chiave esterna per una tabella di dimensioni.

fallire velocemente

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

limite di isolamento dei guasti

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

ramo di funzionalità

Vedi filiale.

caratteristiche

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

importanza delle caratteristiche

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

trasformazione delle funzionalità

Per ottimizzare i dati per il processo di machine learning, incluso l'arricchimento dei dati con fonti aggiuntive, il dimensionamento dei valori o l'estrazione di più set di informazioni da un singolo campo di dati. Ciò consente al modello di ML di trarre vantaggio dai dati. Ad esempio, se suddividi

la data "2021-05-27 00:15:37" in "2021", "maggio", "giovedì" e "15", puoi aiutare l'algoritmo di apprendimento ad apprendere modelli sfumati associati a diversi componenti dei dati.

prompt con pochi scatti

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

FGAC

Vedi il controllo granulare degli accessi.

controllo granulare degli accessi (FGAC)

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

migrazione flash-cut

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

FM

Vedi il modello di base.

modello di fondazione (FM)

Una grande rete neurale di deep learning che si è addestrata su enormi set di dati generalizzati e non etichettati. Le FM sono in grado di eseguire 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.

Gateway FM

Un intermediario centralizzato che controlla e normalizza l'accesso ai modelli di base. Conosciuto anche come gateway LLM.

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

strategia greenfield

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

guardrail

Una regola di livello elevato che consente di governare risorse, policy e conformità tra le unità organizzative (OU). 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 .

guardrail (AI)

Meccanismi di sicurezza che filtrano, convalidano e limitano gli input e gli output degli agenti per contribuire a garantire un comportamento dell'IA responsabile e sicuro.

H

AH

Vedi disponibilità elevata.

migrazione di database eterogenea

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

alta disponibilità (HA)

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

modernizzazione storica

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

dati di esclusione

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

human-in-the-loop (HITL)

Un modello di flusso di lavoro in cui l'esecuzione degli agenti viene sospesa per la revisione e l'approvazione umana nei punti decisionali critici.

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, ad esempio 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 nel Framework. AWS Well-Architected

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. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione per proteggere l'interfaccia bidirezionale tra l'applicazione e Internet in generale.

migrazione incrementale

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

Industria 4.0

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

infrastruttura

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

infrastruttura come codice (IaC)

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

Internet delle cose industriale (IIoT)

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

VPC di ispezione

In un'architettura AWS multi-account, un VPC centralizzato che gestisce le ispezioni del traffico di rete tra VPC (uguali o diversi Regioni AWS), Internet e reti locali. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione 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, consulta 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 gli LLM.

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.

MCP

Vedi Model Context Protocol.

Model Context Protocol (MCP)

Un protocollo stateless per la comunicazione tra agenti e strumenti.

Server MCP

Un servizio che espone uno o più strumenti tramite il Model Context Protocol.

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, vedete 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 da macchina a macchina (M2M) leggero, basato sul publish/subscribemodello, per dispositivi IoT con risorse limitate.

microservizio

Un piccolo servizio indipendente che comunica tramite API ben definite ed è in genere di proprietà di piccoli team autonomi. 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 tramite un'interfaccia ben definita utilizzando API leggere. 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

Cross-functional team 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 da macchina a macchina (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 Framework. AWS Well-Architected

tecnologia operativa (OT)

Sistemi hardware e software che interagiscono con l'ambiente fisico per controllare operazioni, apparecchiature e 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 in tutto tutti i bucket S3 Regioni AWS, la crittografia lato server con AWS KMS (SSE-KMS) e le richieste dinamiche PUT e dirette al bucket S3. 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. Nel documento Architettura di riferimento per la sicurezza di AWS si consiglia di configurare l'account di rete con VPC in entrata, in uscita e di ispezione 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 ingegneristico dei sistemi che tiene conto della privacy durante l'intero processo di sviluppo.

zone ospitate private

Un container che contiene informazioni su come si desidera che Amazon Route 53 risponda alle query DNS per un dominio e i relativi sottodomini all'interno di uno o più VPC. 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 utilizzare Regioni AWS il proprio account.

regressione

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

riospitare

Vedi 7 R.

rilascio

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

trasferisco

Vedi 7 Rs.

ripiattaforma

Vedi 7 Rs.

riacquisto

Vedi 7 Rs.

resilienza

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

policy basata su risorse

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

matrice 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 policy che fornisce il controllo centralizzato sulle autorizzazioni per tutti gli account di un'organizzazione in AWS Organizations. Le SCP definiscono i guardrail o fissano i limiti alle azioni che un amministratore può delegare a utenti o ruoli. Puoi utilizzare le SCP 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.

Shadow AI

Applicazioni di intelligenza artificiale non autorizzate create o utilizzate al di fuori dei canali regolamentati all'interno di un'organizzazione.

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.

modello split-and-seed

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 Modernizzare i servizi Web Microsoft ASP.NET (ASMX) legacy in modo incrementale utilizzando contenitori e Amazon API Gateway.

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

Key-value coppie 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.

strumento

Una funzione o API che un agente può richiamare per eseguire operazioni in sistemi esterni.

Transit Gateway

Un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti on-premise. 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 VPC che consente di instradare il traffico tramite 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 interrogazioni 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.