Guía de seguridad y operaciones del Marco de Datos de Conducción Autónoma (ADDF)

AWS Guía prescriptiva

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Guía prescriptiva: Guía de seguridad y operaciones del Marco de Datos de Conducción Autónoma (ADDF)

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Guía de seguridad y operaciones del Marco de datos de conducción autónoma (ADDF)

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

Noviembre de 2022 (historial de documentos)

Autonomous Driving Data Framework (ADDF) es un proyecto de código abierto diseñado para proporcionar artefactos de código modulares y reutilizables para los equipos de automoción que desean implementar tareas comunes para sistemas avanzados de asistencia al conductor (ADAS), como configurar el almacenamiento de datos centralizado, las canalizaciones de procesamiento de datos, los mecanismos de visualización, las interfaces de búsqueda, las cargas de trabajo de simulación, las interfaces de análisis y los paneles prediseñados. Con ADDF él, puede compartir, modificar o crear módulos totalmente personalizables que reducen el esfuerzo necesario para crear e implementar estas soluciones.

El objetivo de esta guía es ayudarlo a comprender las mejores prácticas para implementar y operar de forma segura ADDF en el Nube de AWS. Se analizan los siguientes temas:

- Arquitectura y terminología: analice la arquitectura general, los flujos de trabajo y los términos importantes.
- Modelo de responsabilidad compartida— Comprenda su función y la función que desempeña a la hora de AWS proteger su ADDF implementación y sus recursos en la nube.
- Proceso de revisión de seguridad— Como ADDF se trata de un proyecto de código abierto, revise cómo AWS y sus colaboradores realizan las revisiones de seguridad.
- Características de seguridad integradas— Revise cómo se integran las mejores prácticas y funciones de seguridad en el proyecto de ADDF código abierto y su marco de implementación.
- Configuración y operación seguras— Aprenda a implementar y operar ADDF en el Nube de AWS.

Destinatarios previstos

Esta guía está destinada a los equipos de operaciones de desarrollo (DevOps), los ingenieros de infraestructura, los administradores, el personal de seguridad de TI y los equipos de respuesta a

incidentes que tienen la tarea de evaluar, implementar, personalizar y operar. ADDF Puede aplicar las recomendaciones de esta guía para nuestros entornos de proof-of-concept producción.

En esta guía se presupone que no tiene conocimientos previos sobreADDF. Sin embargo, le recomendamos que lea el ADDFarchivo readme (GitHub) antes de continuar.

Resultados empresariales específicos

Esta guía está diseñada para ayudarle a configurar y operar con más confianza y seguridad ADDF en entornos de desarrollo y producción.

Arquitectura y terminología del ADDF

Antes de comprender los temas operativos y de seguridad de esta guía, es importante contar con un amplio conocimiento de la terminología, los componentes y la arquitectura del Marco de Datos de Conducción Autónoma (ADDF). Esta sección consta de los siguientes temas:

- Terminología del ADDF
- Arquitectura del ADDF

Terminología del ADDF

La terminología clave del ADDF es la siguiente:

- Módulo de ADDF: un módulo es una infraestructura como código (IaC) que implementa una tarea común en un sistema avanzado de asistencia al conductor (ADAS). Las tareas habituales incluyen la configuración del almacenamiento de datos centralizado, las canalizaciones de procesamiento de datos, los mecanismos de visualización, las interfaces de búsqueda, las cargas de trabajo de simulación, las interfaces de análisis y los paneles prediseñados. Puede crear un módulo en función de sus necesidades o puede reutilizar o personalizar un módulo existente.

  Puede utilizar AWS Cloud Development Kit (AWS CDK) para definir los módulos de ADDF, o utilizar cualquier marco de IaC común, como Hashicorp Terraform o AWS CloudFormation, a fin de implementar los módulos de ADDF. Un módulo cuenta con un conjunto de parámetros de entrada. Los parámetros de entrada pueden depender de los valores de salida de otros módulos. Un módulo de ADDF es la unidad de implementación más pequeña para una Cuenta de AWS de destino del ADDF.
- Archivo de manifiesto de la implementación del ADDF: este archivo define una orquestación de módulos de ADDF independientes. La orquestación hace referencia al orden de implementación de los módulos. En el archivo de manifiesto de la implementación del ADDF, puede utilizar grupos del ADDF para agrupar módulos relacionados. En este archivo, también se define la Cuenta de AWS de la cadena de herramientas del ADDF, las Cuentas de AWS de destino del ADDF y las Regiones de AWS de destino.
- Marco de implementación del ADDF: este marco implementa módulos de ADDF en las Cuentas de AWS de destino del ADDF en función de la orquestación que se define en el archivo de manifiesto

de la implementación del ADDF. El marco de implementación del ADDF se implementa mediante los siguientes proyectos de código abierto de AWS:

- SeedFarmer (GitHub): SeedFarmer es la herramienta de la CLI que se utiliza para las implementaciones del ADDF. Administra el estado de cada módulo, prepara y empaqueta el código del módulo, crea las políticas de privilegio mínimo para los roles de implementación del ADDF y proporciona instrucciones semánticas que CodeSeeder utiliza para la implementación. Puede interactuar directamente con SeedFarmer para ejecutar implementaciones del ADDF o puede integrarlo en una canalización de integración e implementación continuas (CI/CD).
- CodeSeeder (GitHub): CodeSeeder implementa una infraestructura arbitraria como paquetes de código a través de un trabajo de AWS CodeBuild. SeedFarmer orquesta y ejecuta CodeSeeder de forma automática. Solo SeedFarmer interactúa directamente con CodeSeeder.

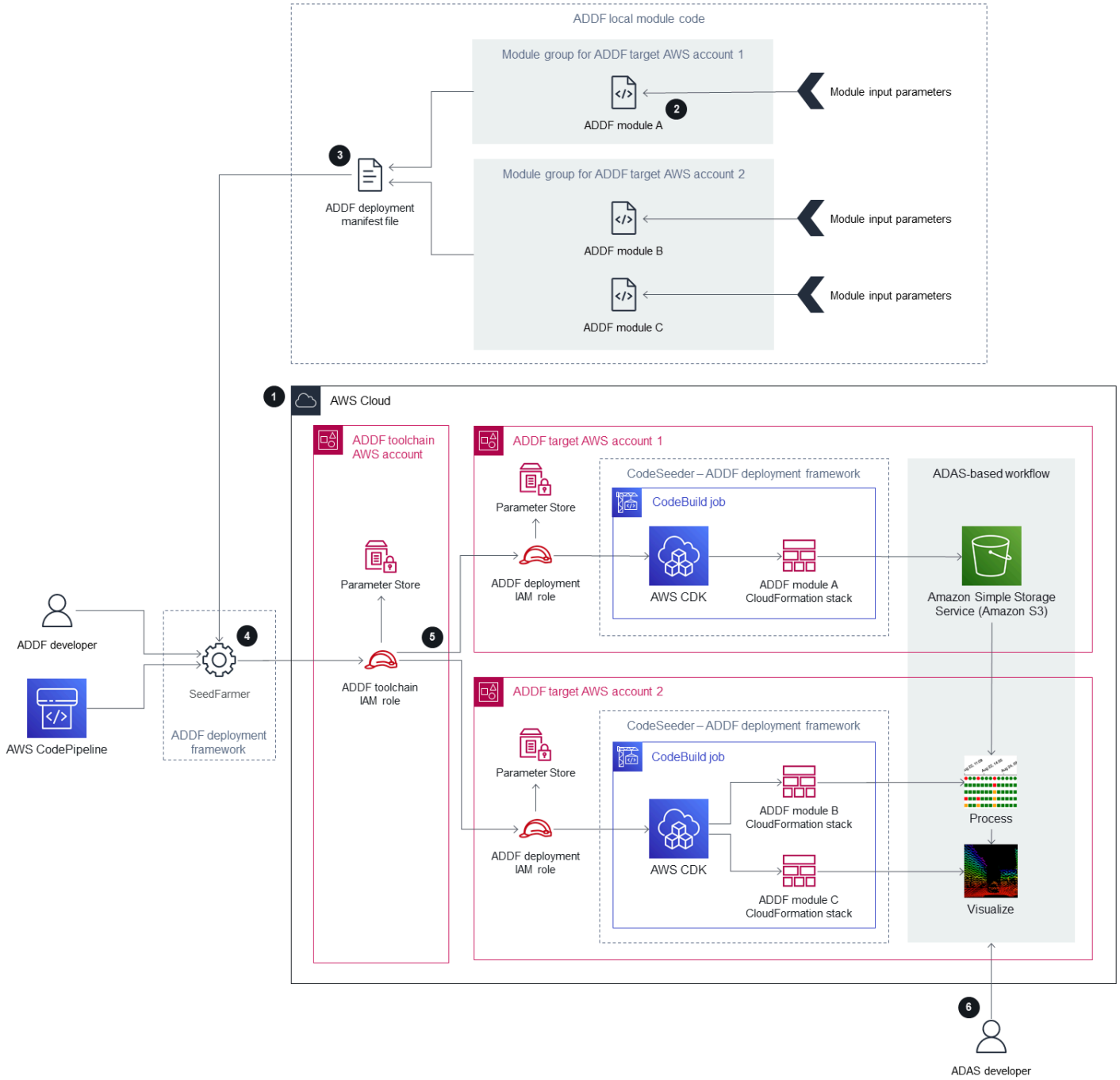
El marco de implementación del ADDF se ha diseñado para admitir las implementaciones en arquitecturas de una y varias cuentas. En función de los requisitos de su organización, decide si se requiere una arquitectura de una o varias cuentas.

- Cuenta de AWS de la cadena de herramientas del ADDF: esta cuenta orquesta y administra la implementación de los módulos en las Cuentas de AWS de destino del ADDF, en función de las definiciones del archivo de manifiesto de la implementación del ADDF. Una implementación del ADDF solo puede tener una Cuenta de AWS de la cadena de herramientas del ADDF. En una arquitectura de una sola cuenta, la Cuenta de AWS de la cadena de herramientas del ADDF también es la Cuenta de AWS de destino del ADDF. Esta cuenta contiene un rol de AWS Identity and Access Management (IAM), denominado rol de IAM de la cadena de herramientas del ADDF, que SeedFarmer asume durante el proceso de implementación del ADDF. En esta guía, nos referimos a una Cuenta de AWS de la cadena de herramientas del ADDF como una cuenta de la cadena de herramientas.
- Cuentas de AWS de destino del ADDF: estas son las cuentas de destino en las que implementará los módulos de ADDF. Puede tener una o más cuentas de destino. Estas cuentas contienen los recursos y la lógica de la aplicación descritos en el archivo de manifiesto de la implementación del ADDF y sus módulos asignados. En una arquitectura de una sola cuenta, la Cuenta de AWS de destino del ADDF también es la Cuenta de AWS de la cadena de herramientas del ADDF. Cada cuenta de destino del ADDF contiene un rol de IAM, denominado Rol de IAM de la implementación del ADDF, que CodeSeeder asume durante el proceso de implementación. En esta guía, nos referimos a una Cuenta de AWS de destino del ADDF como una cuenta de destino.
- Instancia del ADDF: al implementar el ADDF y sus módulos en la nube, como se define en el archivo de manifiesto de la implementación del ADDF, se convierte en una instancia del

ADDF. Una instancia del ADDF puede tener una arquitectura de una o varias cuentas, y puede implementar varias instancias del ADDF. Para obtener más información sobre cómo elegir la cantidad de instancias y diseñar una arquitectura de cuentas para su caso de uso, consulte Definición de la arquitectura del ADDF.

Arquitectura del ADDF

En el siguiente diagrama, se muestra una arquitectura de alto nivel para una instancia del ADDF en la Nube de AWS. Muestra una arquitectura de varias cuentas, que incluye una cuenta de la cadena de herramientas dedicada y dos cuentas de destino. En esta guía, se describe el proceso integral del uso del ADDF para implementar recursos en las cuentas de destino.



1. Cree y arranque las Cuentas de AWS del ADDF.

   Para que funcione de forma correcta, cada cuenta debe arrancarse en el ADDF y AWS CDK. Si se trata de una implementación del ADDF nueva o si agregará cuentas de destino nuevas, realice lo siguiente:

a. Arranque AWS CDK en la cuenta de la cadena de herramientas y en cada cuenta de destino. Para obtener instrucciones, consulte Proceso de arranque (documentación de AWS CDK). ADDF utiliza AWS CDK para implementar su infraestructura.

b. Arranque el ADDF en la cuenta de la cadena de herramientas y en cada cuenta de destino. Para obtener instrucciones, consulte Cuenta de AWS de arranque en la Guía de implementación del ADDF. Esto configura todos los roles de IAM específicos del ADDF que requieren SeedFarmer y CodeSeeder.

> **Note**
>
> Debe realizar este paso solo si implementa el ADDF al principio o agrega cuentas de destino nuevas. Este paso no forma parte de las implementaciones del ADDF recurrentes en instancias del ADDF que ya se han establecido.

2. Cree o personalice los módulos de ADDF.

   Cree o personalice los módulos de ADDF en función del problema específico que intenta resolver. El módulo debe representar una tarea aislada o un grupo de tareas. Defina los parámetros de entrada para el módulo según sea necesario y utilice los valores de salida del módulo como parámetros de entrada para otros módulos.

3. Defina la orquestación del módulo en el archivo de manifiesto de la implementación del ADDF.

   En el archivo de manifiesto del ADDF, organice los módulos en grupos y defina el orden de implementación y las dependencias entre ellos. En este archivo, también debe especificar la cuenta de la cadena de herramientas única y las cuentas de destino (incluido las Regiones de AWS) para cada grupo del ADDF y sus módulos.

4. Evalúe el archivo de manifiesto de la implementación del ADDF y establezca el alcance de la implementación.

   El desarrollador del ADDF o una canalización de CI/CD, como AWS CodePipeline, inicia una evaluación del archivo de manifiesto de la implementación del ADDF al llamar a la herramienta de CLI, SeedFarmer. Para iniciar la evaluación:

   - SeedFarmer utiliza el archivo de manifiesto de la implementación del ADDF como parámetro de entrada para la evaluación.

- Para asumir el rol de IAM de la cadena de herramientas del ADDF, SeedFarmer espera tener el mismo rol de IAM válido o credenciales de usuario que se definieron durante el proceso de arranque del ADDF, en el paso 1.

Si SeedFarmer no cuenta con las credenciales correctas para asumir el rol de IAM de la cadena de herramientas del ADDF o no puede acceder al archivo de manifiesto de la implementación del ADDF, la evaluación no comienza.

Si SeedFarmer puede iniciar la evaluación, asume el rol de IAM de la cadena de herramientas del ADDF en la cuenta de la cadena de herramientas. Desde allí, SeedFarmer puede acceder a cualquier cuenta de destino, al asumir el rol de IAM de la implementación del ADDF en esa cuenta. Luego, SeedFarmer intenta leer todos los metadatos del ADDF en la cuenta de la cadena de herramientas y las cuentas de destino. Se produce una de las circunstancias siguientes:

- Si no hay metadatos del ADDF que leer, eso indica que se trata de una instancia del ADDF nueva. SeedFarmer determina que el alcance de la implementación abarca todo el archivo de manifiesto de la implementación del ADDF y su contenido.
- Si existen metadatos del ADDF, SeedFarmer compara el archivo de manifiesto de la implementación del ADDF y su contenido con los hashes MD5 de los artefactos implementados existentes en las cuentas de destino. Si se detectan cambios que se pueden implementar, este proceso continúa. Si no se detectan cambios que se pueden implementar, el proceso se ha completado.

5. Implemente los módulos del ADDF dentro del alcance en las cuentas de destino.

   Ahora, CodeSeeder cuenta con una lista ordenada de implementaciones que ejecutar, de acuerdo con el archivo de manifiesto de la implementación del ADDF y los resultados de la evaluación del paso anterior. En función de esa lista ordenada, CodeSeeder asume el rol de IAM de la implementación del ADDF en cada cuenta de destino asociada. Luego, ejecuta CodeSeeder en un trabajo de AWS CodeBuild a fin de crear o actualizar las implementaciones de IaC individuales, como aplicaciones de AWS CDK, para el módulo del ADDF. De forma predeterminada, el ADDF utiliza AWS CDK como su marco de IaC, pero también se admiten otros marcos de IaC comunes. Una vez finalizado el proceso para cada cuenta de destino, dispondrá de un flujo de trabajo completamente implementado, entre cuentas e integral basado en el ADAS, como se definió en el archivo de manifiesto de la implementación del ADDF.

   Si utiliza una arquitectura de una sola cuenta, la cuenta de la cadena de herramientas y las cuentas de destino son la misma cuenta y una cuenta tiene todas las funciones descritas.

6. Utilice la infraestructura implementada por el ADDF.

   Un desarrollador del ADAS puede utilizar el flujo de trabajo basado en el ADAS implementado, según lo defina su caso de uso.

   En este flujo de trabajo, se describe la arquitectura de una sola instancia de un entorno de varias cuentas del ADDF. Según su modelo de desarrollo, implementación y operaciones, le recomendamos que ejecute varias instancias del ADDF en un entorno de varias etapas. Una configuración típica podría incluir una instancia del ADDF dedicada con Cuentas de AWS dedicadas para cada etapa de implementación, como ramas para el desarrollo, las pruebas y la producción. También puede ejecutar varias instancias del ADDF en el mismo entorno de una o varias cuentas en la misma Región de AWS, al asumir que creó un espacio de nombres de recursos único para cada instancia del ADDF. Para obtener más información, consulte Definición de la arquitectura del ADDF.

Modelo de responsabilidad compartida del ADDF

El modelo de responsabilidad compartida que se aplica a los Servicios de AWS también se aplica al Marco de Datos de Conducción Autónoma (ADDF). Las siguientes entidades comparten la responsabilidad de proteger el ADDF, tal como se indica en el siguiente diagrama:

- AWS: el proveedor de infraestructura en la nube que ofrece los Servicios de AWS.
- Equipo principal del ADDF: el equipo principal del ADDF es la entidad que publica las versiones del ADDF en el Repositorio del ADDF (GitHub).
- Usuario del ADDF: los usuarios del ADDF incluyen, entre otros:
  - Desarrollador del ADDF: cualquier persona que cambie, personalice o cree un código de módulo del ADDF nuevo.
  - Operador del ADDF: cualquier persona que configure y opere una instancia del ADDF.
  - Desarrollador del ADAS: el usuario final o consumidor de los recursos que implementa el ADDF. Por ejemplo, un desarrollador del ADAS puede consultar una interfaz de visualización que se creó como parte de la implementación del ADDF.

En el siguiente diagrama, se resume la responsabilidad compartida entre AWS, el equipo principal del ADDF y el usuario del ADDF.

AWS responsibility
"Security of the AWS Cloud"

- Software security, including compute, storage, database, and networking
- Hardware security for the AWS global infrastructure, including AWS Regions, Availability Zones, and edge locations

ADDF core team responsibility
"Security-hardened framework on an as-is basis, as stated in Apache License 2.0"

- Periodic security reviews of releases
- Baseline security features
- Security-hardened default modules*
- Security-hardened deployment and orchestration framework

ADDF user responsibility
"Secure setup, development, customization, and operation"

- General AWS account responsibilities:
  - Security controls and checks (directive, detective, preventive, and responsive)
  - Multi-account architecture
  - Networking design
  - Identity and access management
- ADDF responsibilities:
  - ADDF setup
  - ADDF customization
  - ADDF module development
  - ADDF operations
  - ADDF updates

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

Responsabilidad de AWS

AWS es responsable de proteger la infraestructura en la que se ejecutan todos los servicios que se ofrecen en la Nube de AWS, tal como se define en el Modelo de responsabilidad compartida de AWS. Esta infraestructura está conformada por el equipo, el software, las redes y las instalaciones que ejecutan servicios de la Nube de AWS.

Responsabilidad del equipo principal del ADDF

El equipo principal del ADDF ofrece un marco que es seguro en sí mismo, en la medida de lo posible, en función de la Licencia Apache 2.0 (GitHub). El equipo principal del ADDF es responsable de lo siguiente:

- Revisiones de seguridad periódicas de las versiones
- Características de seguridad de referencia
- Módulos predeterminados con seguridad reforzada (se excluyen los módulos de la carpeta `/modules/demo-only/`. Estos módulos solo son para fines de prueba de concepto y no reciben ningún refuerzo de seguridad).
- Marco de implementación y orquestación con seguridad reforzada

Estas responsabilidades de seguridad solo se extienden al marco, tal como se proporciona en el repositorio de GitHub, sin modificaciones ni personalizaciones. Esto incluye todos los módulos del ADDF, excepto los de la carpeta `modules/demo-only/`. Los módulos del ADDF de esta carpeta no cuentan con seguridad reforzada y no se deberían implementar en entornos de producción ni en ningún entorno con datos confidenciales o protegidos. Estos módulos se incluyen para mostrar las capacidades del sistema y puede utilizarlos como base para crear sus propios módulos personalizados y con seguridad reforzada.

> **Note**
>
> El ADDF como marco se brinda “tal cual”. No conlleva ninguna responsabilidad ni garantía, tal y como se indica en la Licencia Apache 2.0 (GitHub). Debe realizar su propia evaluación de seguridad del ADDF y comprobar que cumple con los requisitos de seguridad específicos de su organización.

Responsabilidad del usuario del ADDF

El ADDF y sus módulos son seguros solo si el ADDF se configura, personaliza y opera de forma segura. El usuario del ADDF es completamente responsable de la seguridad de lo siguiente:

- Responsabilidades de la Cuenta de AWS generales:

  - Comprobaciones y controles de seguridad (normativos, de detección, preventivos y de respuesta)
  - Arquitectura de varias cuentas
  - Diseño de redes
  - Administración de identidades y accesos
- Responsabilidades específicas del ADDF:
  - Configuración del ADDF
  - Personalización del ADDF
  - Desarrollo de módulos del ADDF
  - Operaciones del ADDF
  - Actualizaciones del ADDF

Responsabilidades de la Cuenta de AWS generales

Antes de implementar cualquier recurso relacionado con el ADDF en las Cuentas de AWS, se debe configurar sus Cuentas de AWS de acuerdo con las prácticas recomendadas del Marco de AWS Well-Architected. Esto incluye controles de seguridad normativos, de detección, preventivos y de respuesta. Debe contar con procesos de mitigación detallados en caso de que se produzcan vulneraciones o incidentes de seguridad. La política de su organización debe incluir requisitos para administrar de forma centralizada la identidad, el acceso y las redes. Por lo general, un equipo dedicado a la zona de aterrizaje gestiona estos requisitos y servicios.

Responsabilidades específicas del ADDF

Configuración del ADDF segura

La responsabilidad de un usuario del ADDF comienza con la configuración segura del ADDF de acuerdo con la documentación del ADDF. Le recomendamos encarecidamente que siga las instrucciones de la Guía de implementación del ADDF (GitHub). Para obtener más información sobre la configuración segura del ADDF, consulte Definición de la arquitectura del ADDF y Configuración inicial.

Personalización del ADDF segura

En caso de personalizar funciones principales del ADDF, como CodeSeeder, SeedFarmer y los módulos principales del ADDF, el usuario del ADDF asume toda la responsabilidad por dichos

cambios. Para obtener más información, consulte Personalización del código de marco de implementación del ADDF.

Desarrollo de módulos del ADDF seguro

El usuario del ADDF es completamente responsable de cualquier módulo personalizado que se implemente mediante ADDF. Además, el usuario del ADDF es responsable de cualquier cambio de código en los módulos que suministra el ADDF. Para obtener más información, consulte Escritura de módulos personalizados en el ADDF.

Actualizaciones y operaciones del ADDF seguras

A medida que el marco evoluciona, el ADDF recibe actualizaciones de características y seguridad. Es responsabilidad del usuario del ADDF comprobar de forma periódica las actualizaciones que se publican en el repositorio de GitHub y operar el ADDF de manera segura a largo plazo. Para obtener más información, consulte Implementaciones del ADDF recurrentes, Auditorías de seguridad recurrentes, Actualizaciones del ADDF y Desactivación.

Proceso de revisión de seguridad del ADDF

El Marco de Datos de Conducción Autónoma (ADDF) se creó en función de la seguridad. Antes de su lanzamiento al público, AWS realizó una revisión inicial de seguridad interna del ADDF y resolvió cualquier problema de seguridad identificado. Tanto AWS como la comunidad de código abierto contribuyen a las revisiones de seguridad continuas del marco.

Revisiones de seguridad periódicas realizadas por AWS

El ADDF se publica bajo la organización de GitHub awslabs que es propiedad de AWS. AWS realiza revisiones de seguridad automáticas y manuales periódicas del código de esta organización para verificar la seguridad en la medida de lo posible. Según la política de AWS, AWS no divulga información sobre la frecuencia, el enfoque o las herramientas de las revisiones de seguridad utilizadas. Además, AWS no publica ningún informe de auditoría interna sobre el ADDF. Sin embargo, cualquier resultado de seguridad identificado se corrige y se publica a través de una solicitud de extracción, con suma urgencia.

> **Note**
>
> El ADDF, como marco, se entrega “TAL CUAL”, SIN GARANTÍAS NI CONDICIONES DE NINGÚN TIPO, ya sean expresas o implícitas, incluidas, entre otras, las garantías o condiciones de propiedad, no infracción, comerciabilidad o idoneidad para un propósito determinado, tal como se establece en la Licencia Apache 2.0 (GitHub). Debe realizar su propia evaluación de seguridad del ADDF y comprobar si cumple con los requisitos de seguridad específicos de su organización, tal como se establece en la Licencia Apache 2.0. Es el único responsable de determinar si es apropiado utilizar o redistribuir el ADDF y asumir cualquier riesgo asociado al ejercicio o a los permisos que se le concedan en virtud de dicha licencia.

Contribuciones y revisiones de seguridad de código abierto

El ADDF es un proyecto de código abierto que acepta contribuciones. Invitamos a todos los usuarios a realizar su propia revisión de seguridad del marco y a contribuir al informar sobre cualquier resultado relacionado con la seguridad. Si encuentra algún problema en el código, siga las directrices en Notificaciones de problemas de seguridad (documentación del ADDF).

Características de seguridad integradas del ADDF

El Marco de Datos de Conducción Autónoma (ADDF) cuenta con varias características de seguridad integradas. De forma predeterminada, estas características se han diseñado para ayudarlo a configurar un marco seguro y ayudar a su organización a cumplir los requisitos de seguridad empresariales más comunes.

Las siguientes son las características de seguridad integradas:

- Privilegio mínimo para el código de módulo del ADDF
- Infraestructura como código
- Controles de seguridad automatizados para la IaC
- Política de privilegio mínimo personalizada para rol de implementación de AWS CDK
- Política de privilegio mínimo para el archivo deployspec del módulo
- Cifrado de datos
- Almacenamiento de credenciales mediante Secrets Manager
- Revisiones de seguridad de SeedFarmer y CodeSeeder
- Compatibilidad con el límite de permisos para el rol de AWS CodeBuild de CodeSeeder
- Arquitectura de varias cuentas de AWS
- Permisos de privilegio mínimo para implementaciones con varias cuentas

Privilegio mínimo para el código de módulo del ADDF

El privilegio mínimo es la práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte Aplicar permisos de privilegio mínimo. Los módulos que proporciona el ADDF siguen de forma rigurosa el principio de privilegio mínimo en su código y en los recursos implementados, de la siguiente manera:

- Todas las políticas de AWS Identity and Access Management (IAM) que se generan para un módulo de ADDF cuentan con los permisos mínimos necesarios para cada caso de uso.
- Los Servicios de AWS se configuran e implementan de acuerdo con el principio de privilegio mínimo. Los módulos que proporciona el ADDF solo utilizan los servicios y las características de servicio necesarios para el caso de uso específico.

Infraestructura como código

El ADDF, como marco, se ha diseñado para implementar los módulos de ADDF como infraestructura como código (IaC). La IaC elimina los procesos de implementación manual y ayuda a prevenir errores y configuraciones incorrectas, que pueden resultar de procesos manuales.

El ADDF se ha diseñado para orquestar e implementar módulos mediante cualquier marco de IaC común. Esto incluye, entre otros:

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

Puede utilizar diferentes marcos de IaC para escribir distintos módulos y, luego, utilizar el ADDF para implementarlos.

El marco de IaC predeterminado que utilizan los módulos de ADDF es AWS CDK. AWS CDK es una abstracción de alto nivel orientada a objetos que se puede utilizar para definir recursos de AWS imperativamente. AWS CDK ya aplica las prácticas recomendadas de seguridad de forma predeterminada para varios servicios y escenarios. Mediante el uso de AWS CDK, se reduce el riesgo de errores de configuración de seguridad.

Controles de seguridad automatizados para la IaC

La utilidad cdk-nag (GitHub) de código abierto se encuentra integrada en el ADDF. Esta utilidad comprueba de forma automática los módulos de ADDF que se basan en AWS CDK para el cumplimiento de las prácticas recomendadas generales y de seguridad. La utilidad cdk-nag utiliza reglas y paquetes de reglas para detectar y denunciar el código que infringe las prácticas recomendadas. Para obtener más información sobre las reglas y una lista completa, consulte Reglas de cdk-nag (GitHub).

Política de privilegio mínimo personalizada para rol de implementación de AWS CDK

El ADDF hace un uso extensivo de AWS CDK v2. Es necesario que arranque todas las Cuentas de AWS en AWS CDK del ADDF. Para obtener más información, consulte Proceso de arranque (documentación de AWS CDK).

De forma predeterminada, AWS CDK asigna AdministratorAccess, la política administrada por AWS permisiva, al rol de implementación de AWS CDK creado en cuentas de arranque. El nombre completo de este rol es `cdk-[CDK_QUALIFIER]-cfn-exec-role-[AWS_ACCOUNT_ID]-[REGION]`. AWS CDK utiliza este rol para implementar recursos en la Cuenta de AWS de arranque como parte del proceso de implementación de AWS CDK.

En función de los requisitos de seguridad de su organización, la política `AdministratorAccess` puede ser demasiado permisiva. Como parte del proceso de arranque de AWS CDK, puede personalizar la política y los permisos según sus necesidades. Puede cambiar la política al reiniciar el arranque de la cuenta con una política recién definida mediante el parámetro `--cloudformation-execution-policies`. Para obtener más información, consulte Personalización del proceso de arranque (documentación de AWS CDK).

> **Note**
>
> Si bien esta característica de seguridad no es específica del ADDF, aparece en esta sección porque puede aumentar la seguridad general de la implementación del ADDF.

Política de privilegio mínimo para el archivo deployspec del módulo

Cada módulo contiene un archivo de especificaciones de la implementación que se denomina deployspec.yaml. Este archivo define las instrucciones de implementación del módulo. CodeSeeder lo utiliza para implementar el módulo definido en la cuenta de destino mediante AWS CodeBuild. CodeSeeder asigna un rol de servicio predeterminado a CodeBuild para implementar los recursos, como se indica en el archivo de especificaciones de la implementación. Este rol de servicio se ha diseñado en función del principio de privilegio mínimo. Incluye todos los permisos necesarios para la implementación de aplicaciones de AWS CDK, ya que todos los módulos que proporciona el ADDF se crean como aplicaciones de AWS CDK.

Sin embargo, si necesita ejecutar algún comando de etapa fuera de AWS CDK, debe crear una política de IAM personalizada en lugar de utilizar el rol de servicio predeterminado para CodeBuild. Por ejemplo, si utiliza un marco de implementación de IaC que no sea AWS CDK, como Terraform, debe crear una política de IAM que conceda los permisos suficientes para que funcione ese marco específico. Otro escenario que requiere una política de IAM específica es cuando incluye llamadas a AWS Command Line Interface (AWS CLI) directas a otros Servicios de AWS en los comandos de etapa `install`, `pre_build`, `build` o `post_build`. Por ejemplo, necesita una política personalizada si su módulo incluye un comando de Amazon Simple Storage Service (Amazon S3) para cargar archivos a un bucket de S3. La política de IAM personalizada proporciona un control detallado para cualquier comando de AWS fuera de la implementación de AWS CDK. Para ver un ejemplo de política de IAM personalizada, consulte ModuleStack (documentación de SeedFarmer). Al crear una política de IAM personalizada para su módulo de ADDF, asegúrese de aplicar los permisos de privilegio mínimo.

Cifrado de datos

El ADDF almacena y procesa datos potencialmente confidenciales. A fin de ayudar a proteger estos datos, los módulos que proporciona el ADDF, SeedFarmer, CodeSeeder cifran los datos en reposo y en tránsito para todos los Servicios de AWS utilizados (a menos que se indique explícitamente lo contrario para los módulos de la carpeta `demo-only`).

Almacenamiento de credenciales mediante Secrets Manager

ADDF gestiona varios secretos para diferentes servicios, como Docker Hub, JupyterHub y Amazon Redshift. ADDF utiliza AWS Secrets Manager para almacenar cualquier secreto relacionado con el ADDF. Esto lo ayuda a eliminar los datos confidenciales del código fuente.

Los secretos de Secrets Manager solo se almacenan en las cuentas de destino, según sea necesario para que la cuenta funcione de forma correcta. De forma predeterminada, la cuenta de cadena de herramientas no contiene secretos.

Revisiones de seguridad de SeedFarmer y CodeSeeder

SeedFarmer y CodeSeeder (repositorios de GitHub) se utilizan para implementar el ADDF y sus módulos. Estos proyectos de código abierto se someten al mismo proceso regular de revisión de seguridad interna de AWS que ADDF, como se describe en Proceso de revisión de seguridad del ADDF.

Compatibilidad con el límite de permisos para el rol de AWS CodeBuild de CodeSeeder

Los límites de permisos de IAM son un mecanismo de seguridad común que define los permisos máximos que una política basada en identidades puede conceder a una entidad de IAM. SeedFarmer y CodeSeeder permiten adjuntar un límite de permisos de IAM para cada cuenta de destino. El límite de permisos limita los permisos máximos de cualquier rol de servicio que utiliza CodeBuild cuando CodeSeeder implementa módulos. Un equipo de seguridad debe crear los límites de permisos de IAM fuera del ADDF. Los archivos adjuntos de la política de límite de permisos de IAM se aceptan como un atributo dentro del archivo de manifiesto de la implementación del ADDF, deployment.yaml. Para obtener más información, consulte Compatibilidad con el límite de permisos (documentación de SeedFarmer).

El flujo de trabajo es el siguiente:

1. Su equipo de seguridad define y crea un límite de permisos de IAM en función de sus requisitos de seguridad. El límite de permisos de IAM debe crearse de forma individual en cada Cuenta de AWS del ADDF. El resultado es una lista de nombre de recurso de Amazon (ARN) de la política de límite de permisos.
2. El equipo de seguridad comparte la lista de ARN de la política con su equipo de desarrolladores del ADDF.
3. El equipo de desarrolladores del ADDF integra la lista de ARN de la política en el archivo de manifiesto. Para ver un ejemplo de esta integración, consulte sample-permissionboundary.yaml (GitHub) y Manifiesto de implementación (documentación de SeedFarmer).
4. Tras una implementación exitosa, el límite de permisos se adjunta a todos los roles de servicio que CodeBuild utiliza para implementar los módulos.
5. El equipo de seguridad monitorea que los límites de permisos se apliquen según sea necesario.

Arquitectura de varias cuentas de AWS

Tal como se define en el pilar de seguridad del Marco de AWS Well-Architected, se considera una práctica recomendada separar los recursos y las cargas de trabajo en varias Cuentas de AWS, en función de los requisitos de su organización. Esto se debe a que una Cuenta de AWS actúa como límite de aislamiento. Para obtener más información, consulte Administración y separación de Cuenta de AWS. La implementación de este concepto se denomina arquitectura de varias cuentas.

Un diseño adecuado de la arquitectura de varias cuentas de AWS permite categorizar la carga de trabajo y reduce el alcance del impacto en caso de una brecha de seguridad, en comparación con una arquitectura de una sola cuenta.

El ADDF admite de forma nativa arquitecturas de varias cuentas de AWS. Puede distribuir sus módulos de ADDF entre tantas Cuentas de AWS según sea necesario para cumplir con los requisitos de seguridad y separación de funciones de su organización. Puede implementar el ADDF en una sola Cuenta de AWS, al combinar la cadena de herramientas y las funciones de la cuenta de destino. Como alternativa, puede crear cuentas de destino individuales para los módulos o grupos de módulos del ADDF.

La única restricción que debe tener en cuenta es que un módulo de ADDF representa la unidad de implementación más pequeña de cada Cuenta de AWS.

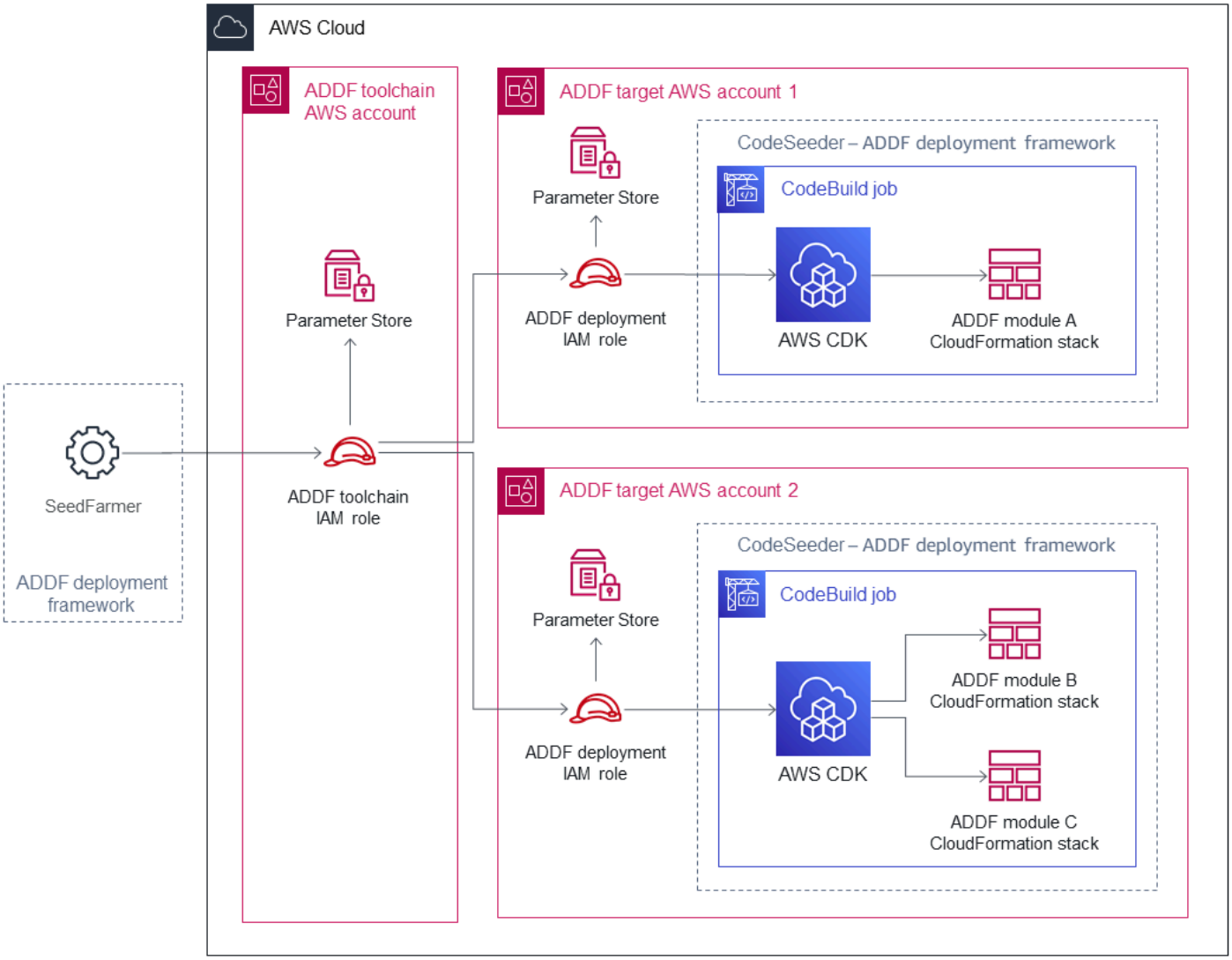
En el caso de los entornos de producción, se recomienda utilizar una arquitectura de varias cuentas compuesta por una cuenta de cadena de herramientas y al menos una cuenta de destino. Para obtener más información, consulte Arquitectura del ADDF.

Permisos de privilegio mínimo para implementaciones con varias cuentas

Si utiliza una arquitectura de varias cuentas, SeedFarmer necesita acceder a las cuentas de destino para realizar las siguientes tres acciones:

1. Escribir los metadatos del módulo de ADDF en la cuenta de cadena de herramientas y en las cuentas de destino.
2. Leer los metadatos del módulo de ADDF de la cuenta de cadena de herramientas y de las cuentas de destino.
3. Iniciar trabajos de AWS CodeBuild en las cuentas de destino, con el fin de implementar o actualizar los módulos.

En la siguiente figura, se muestran las relaciones entre cuentas, incluidas las operaciones para asumir roles de AWS Identity and Access Management (IAM) específicos del ADDF.



Estas acciones entre cuentas se logran mediante el uso de operaciones de asunción de roles bien definidas.

- El rol de IAM de la cadena de herramientas del ADDF se implementa en la cuenta de cadena de herramientas. SeedFarmer asume este rol. Este rol tiene permisos para realizar una acción `iam:AssumeRole` y puede asumir el rol de IAM de implementación del ADDF en cada cuenta de destino. Además, el rol de IAM de la cadena de herramientas del ADDF puede ejecutar operaciones de Almacén de parámetros de AWS Systems Manager locales.
- El rol de IAM de implementación del ADDF se implementa en cada cuenta de destino. Este rol solo se puede asumir desde la cuenta de cadena de herramientas mediante el rol de IAM de la cadena de herramientas del ADDF. Este rol tiene permisos para ejecutar operaciones de Almacén

de parámetros de AWS Systems Manager locales y ejecutar acciones de AWS CodeBuild que inician y describen los trabajos de CodeBuild a través de CodeSeeder.

Estos roles de IAM específicos del ADDF se crean como parte del proceso de arranque del ADDF. Para obtener más información, consulte Cuenta de AWS de arranque en la Guía de implementación del ADDF (GitHub).

Todos los permisos entre cuentas se configuran de acuerdo con el principio de privilegio mínimo. Si una cuenta de destino se ve comprometida, el impacto en las demás Cuentas de AWS del ADDF es mínimo o nulo.

En el caso de una arquitectura de una sola cuenta para el ADDF, las relaciones del rol siguen siendo las mismas. Simplemente se comprimen en una sola Cuenta de AWS.

Configuración y operación seguras del ADDF

El Marco de Datos de Conducción Autónoma (ADDF) debe tratarse como un software personalizado que requiere mantenimiento y cuidado continuos por parte de un equipo dedicado de DevOps y seguridad de su organización. En esta sección, se describen las tareas comunes relacionadas con la seguridad que lo ayudan a configurar y utilizar el ADDF durante todo su ciclo de vida.

Esta sección incluye las siguientes tareas:

- Definición de la arquitectura del ADDF
- Configuración inicial
- Personalización del código de marco de implementación del ADDF
- Escritura de módulos personalizados en el ADDF
- Implementaciones del ADDF recurrentes
- Auditorías de seguridad recurrentes
- Actualizaciones del ADDF
- Desactivación

Definición de la arquitectura del ADDF

Una instancia del ADDF es tan segura como el entorno de la Cuenta de AWS en el que se implementa. Este entorno de la Cuenta de AWS debe diseñarse para satisfacer las necesidades operativas y de seguridad de su caso de uso específico. Por ejemplo, las tareas y consideraciones relacionadas con la seguridad y las operaciones para configurar una instancia del ADDF en un entorno de prueba de concepto (PoC) son diferentes a las de configurar un ADDF en un entorno de producción.

Ejecución del ADDF en un entorno de PoC

Si tiene la intención de utilizar el ADDF en un entorno de PoC, le recomendamos que cree una Cuenta de AWS dedicada para un ADDF que no contenga ninguna otra carga de trabajo. Esto ayuda a mantener su cuenta segura mientras explora el ADDF y sus características. Los siguientes son beneficios de este enfoque:

- En caso de un error de configuración del ADDF grave, ninguna otra carga de trabajo se vería afectada de forma adversa.
- No hay riesgo de que se produzca ningún otro error de configuración de la carga de trabajo que pueda afectar de forma negativa a la configuración del ADDF.

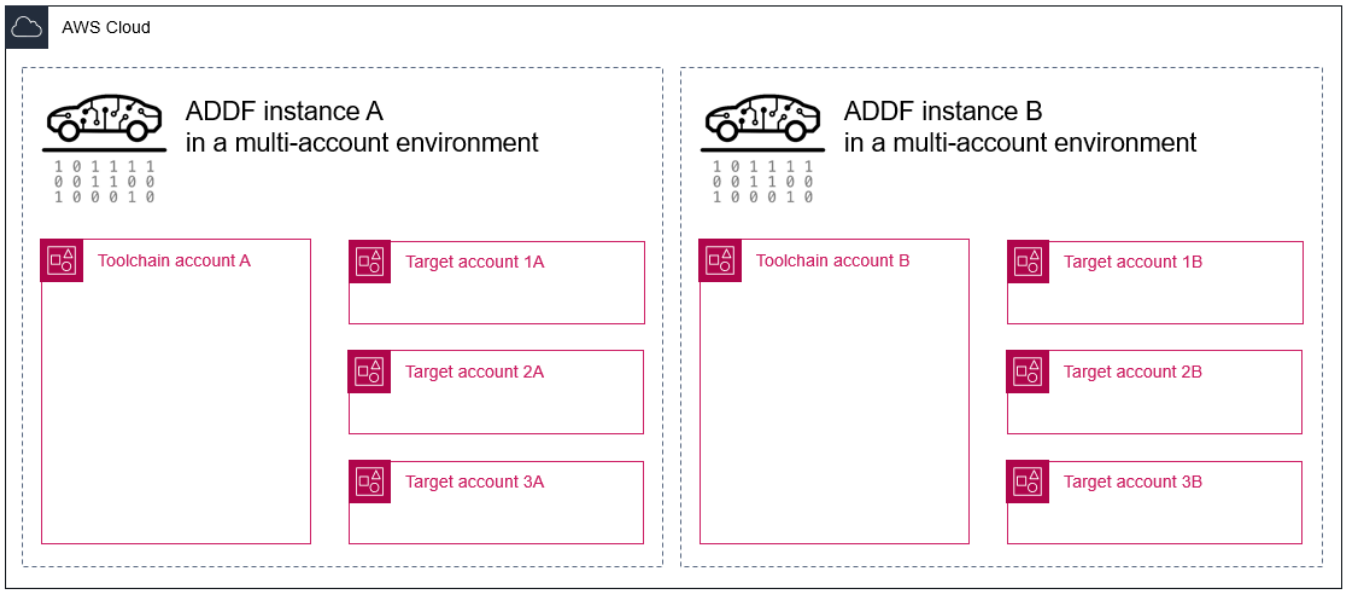
Incluso en el caso de un entorno de PoC, le recomendamos que siga la mayor cantidad posible de prácticas recomendadas que se indican en Ejecución del ADDF en un entorno de producción.

Ejecución del ADDF en un entorno de producción

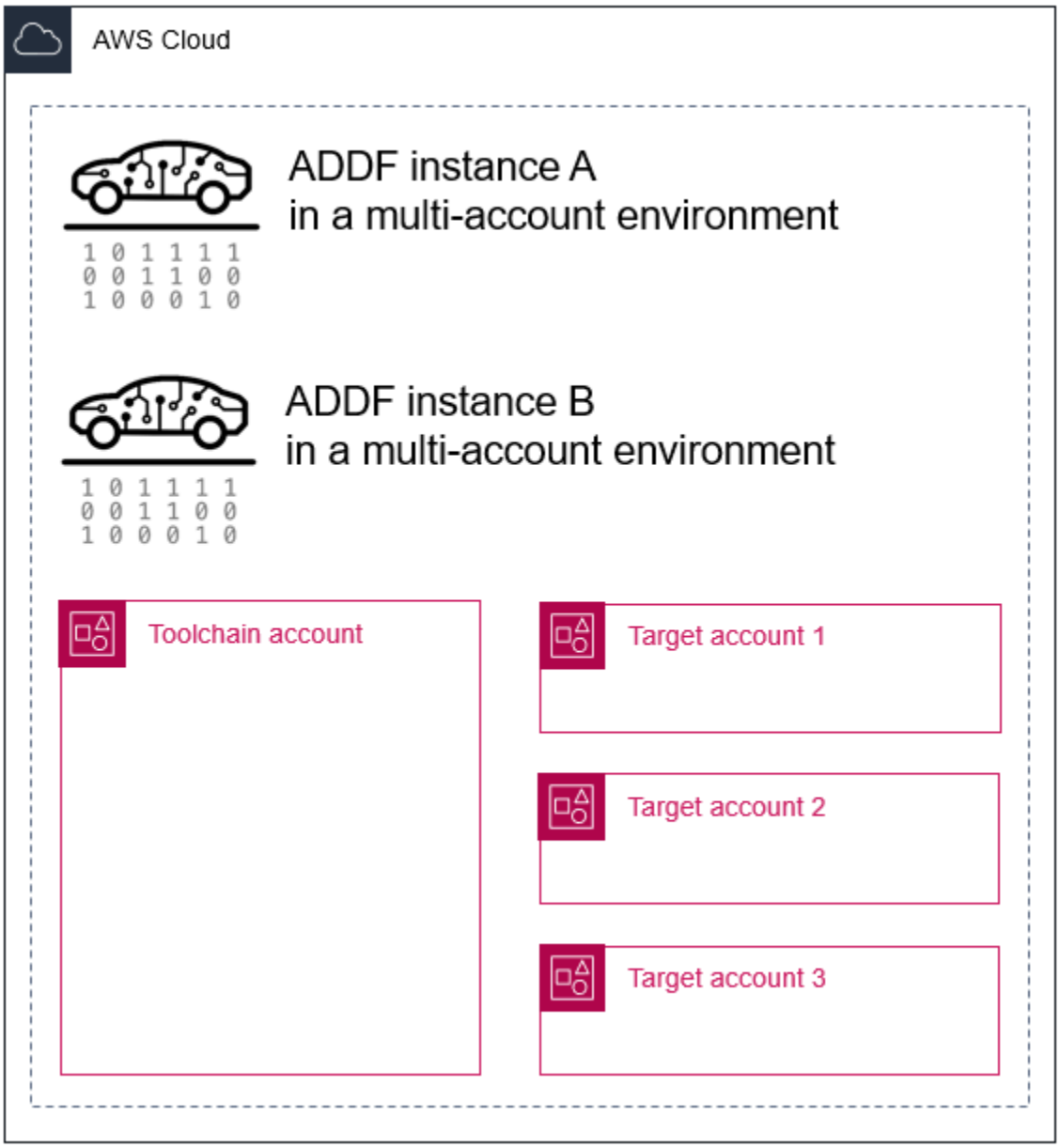
Si tiene la intención de utilizar el ADDF en un entorno de producción empresarial, le recomendamos encarecidamente que tenga en cuenta las prácticas recomendadas de seguridad de su organización e implemente el ADDF en consecuencia. Además de las prácticas recomendadas de seguridad de su organización, le recomendamos que implemente lo siguiente:

- Cree un equipo de DevOps del ADDF comprometido y a largo plazo: el ADDF debe tratarse como un software personalizado. Requiere mantenimiento y cuidados continuos por parte de un equipo de DevOps dedicado. Antes de empezar a ejecutar el ADDF en un entorno de producción, se debe definir un equipo de DevOps con el tamaño y las capacidades suficientes, con un compromiso total de recursos, hasta el final de la vida útil de la implementación del ADDF.
- Utilice una arquitectura de varias cuentas: cada instancia del ADDF debe implementarse en su propio entorno de varias cuentas de AWS dedicado, sin otras carga de trabajo no relacionadas. Tal como se define en la Administración y separación de cuentas de AWS (Marco de AWS Well-Architected), se considera una práctica recomendada separar los recursos y las cargas de trabajo en varias Cuentas de AWS, en función de los requisitos de su organización. Esto se debe a que una Cuenta de AWS actúa como límite de aislamiento. Un diseño adecuado de la arquitectura de varias cuentas de AWS permite categorizar la carga de trabajo y reduce el alcance del impacto en caso de una brecha de seguridad, en comparación con una arquitectura de una sola cuenta. El uso de una arquitectura de varias cuentas también ayuda a que sus cuentas permanezcan dentro de sus Cuotas del Servicio de AWS. Distribuya sus módulos de ADDF entre tantas Cuentas de AWS según sea necesario para cumplir con los requisitos de seguridad y separación de funciones de su organización.
- Implemente varias instancias del ADDF: configure tantas instancias del ADDF independientes como necesite para desarrollar, probar e implementar de forma correcta los módulos del ADDF de acuerdo con los procesos de desarrollo de software de su organización. Al configurar varias instancias del ADDF, puede utilizar uno de los siguientes enfoques:

- Varias instancias del ADDF en diferentes entornos de varias cuentas de AWS: puede utilizar Cuentas de AWS independientes para aislar diferentes instancias del ADDF. Por ejemplo, si su organización cuenta con etapas específicas de desarrollo, pruebas y producción, puede crear instancias del ADDF independientes y cuentas dedicadas para cada etapa. Esto ofrece muchas ventajas, como reducir el riesgo de que cualquier error se propague entre las etapas, ayudarlo a implementar un proceso de aprobación y restringir el acceso de los usuarios solo a determinados entornos. En la siguiente imagen, se muestran dos instancias del ADDF implementadas en entornos independientes de varias cuentas.



- Varias instancias del ADDF en el mismo entorno de varias cuentas de AWS: puede crear varias instancias del ADDF que compartan el mismo entorno de varias cuentas de AWS. Esto crea de manera efectiva ramas aisladas en las mismas Cuentas de AWS. Por ejemplo, si diferentes desarrolladores trabajan en paralelo, un desarrollador puede crear una instancia del ADDF dedicada en las mismas Cuentas de AWS. Esto ayuda a los desarrolladores a trabajar en ramas aisladas con fines de desarrollo y pruebas. Si utiliza este enfoque, para cada instancia del ADDF, sus recursos del ADDF deben tener nombres de recursos únicos. De forma predeterminada, esto se admite en los módulos del ADDF suministrados previamente. Puede utilizar este enfoque siempre que no exceda las Cuotas del Servicio de AWS. En la siguiente imagen, se muestran dos instancias del ADDF implementadas en un entorno compartido de varias cuentas.



- Varias instancias del ADDF en el mismo entorno de una sola cuenta de AWS: esta arquitectura es muy similar a la del ejemplo anterior. La diferencia es que las varias instancias del ADDF se implementan en un entorno de una sola cuenta en lugar de en un entorno de varias cuentas. Esta arquitectura puede adaptarse a casos de uso del ADDF muy simples que tienen un alcance limitado y a varios desarrolladores que trabajan en diferentes ramas a la vez.

Como SeedFarmer es la única herramienta que controla las implementaciones de una instancia del ADDF, puede crear cualquier entorno y arquitectura de cuentas que se adapte a la estrategia de implementación y a los procesos de CI/CD de su organización.

- Personalice el proceso de arranque de AWS Cloud Development Kit (AWS CDK) de acuerdo con los requisitos de seguridad de su organización: de forma predeterminada, AWS CDK asigna la política administrada de AWS AdministratorAccess durante el proceso de arranque. Esta política concede privilegios administrativos completos. Si esta política es demasiado permisiva para los requisitos de seguridad de su organización, puede personalizar las políticas que se aplican. Para obtener más información, consulte Política de privilegio mínimo personalizada para rol de implementación de AWS CDK.
- Siga las prácticas recomendadas al configurar el acceso en IAM: establezca una solución de acceso a AWS Identity and Access Management (IAM) estructurada que permita a sus usuarios acceder a las Cuentas de AWS del ADDF. El marco del ADDF se ha diseñado para cumplir con el principio de privilegio mínimo. Su patrón de acceso a IAM también debe seguir el principio

de privilegio mínimo, debe cumplir con los requisitos de su organización y debe cumplir con las Prácticas recomendadas de seguridad en IAM (documentación de IAM).

- Configure las redes de acuerdo con las prácticas recomendadas de su organización: el ADDF incluye una pila de AWS CloudFormation de redes opcional que crea una nube privada virtual (VPC) pública o privada básica. Según la configuración de su organización, esta VPC podría exponer los recursos directamente a Internet. Le recomendamos que siga las prácticas recomendadas de redes de su organización y cree un módulo de red personalizado con seguridad reforzada.
- Implemente medidas de prevención, detección y mitigación de la seguridad en el nivel de Cuenta de AWS: AWS ofrece varios servicios de seguridad, como Amazon GuardDuty, AWS Security Hub, Amazon Detective y AWS Config. Habilite esos servicios en su Cuenta de AWS del ADDF e integre los procesos de prevención, detección, mitigación y gestión de incidentes de seguridad de su organización. Le recomendamos que siga las Prácticas recomendadas de seguridad, identidad y conformidad (Centro de arquitectura de AWS) y cualquier sugerencia específica de un servicio incluida en la documentación de ese servicio. Para obtener más información, consulte Documentación de seguridad de AWS.

El ADDF no aborda ninguno de estos temas porque los detalles de implementación y configuración dependen en gran medida de los requisitos y procesos específicos de su organización. Por el contrario, es responsabilidad fundamental de su organización abordar estos temas. Por lo general, el equipo que administra su Zona de aterrizaje de AWS lo ayuda a planificar e implementar su entorno del ADDF.

Configuración inicial

Configure el ADDF de acuerdo con la Guía de implementación del ADDF (GitHub). El punto de partida de cualquier implementación es la carpeta `/manifest` en el repositorio de GitHub autonomous-driving-data-framework. La carpeta `/manifest/example-dev` contiene un ejemplo de implementación con fines de demostración. Utilice este ejemplo como punto de partida para diseñar su propia implementación. En ese directorio, hay un archivo de manifiesto de la implementación del ADDF denominado deployment.yaml. Contiene toda la información necesaria para que SeedFarmer administre, implemente o elimine el ADDF y sus recursos en la Nube de AWS. Puede crear grupos de módulos de ADDF en archivos dedicados. El archivo core-modules.yaml es un ejemplo del grupo de módulos principales e incluye todos los módulos principales que proporciona el ADDF. Para

resumir, el archivo deployment.yaml contiene todas las referencias a los grupos y módulos que se implementarán en sus cuentas de destino y especifica el orden de implementación.

Para una configuración segura y compatible, en especial en un entorno que no es una prueba de concepto, le recomendamos que analice el código fuente de cada módulo que desee implementar. De acuerdo con las prácticas recomendadas de refuerzo de la seguridad, solo debe implementar los módulos que sean necesarios para su caso de uso previsto.

> **Note**
>
> Los módulos del ADDF en la carpeta `modules/demo-only/` no cuentan con seguridad reforzada y no se deberían implementar en entornos de producción ni en ningún entorno con datos confidenciales o protegidos. Estos módulos se incluyen para mostrar las capacidades del sistema y puede utilizarlos como base para crear sus propios módulos personalizados y con seguridad reforzada.

Personalización del código de marco de implementación del ADDF

El marco de implementación del ADDF y su lógica de orquestación e implementación se pueden personalizar por completo para cumplir con cualquier requisito. Sin embargo, le sugerimos que se abstenga de personalizar estas funciones o minimice los cambios por los siguientes motivos:

- Mantenga la compatibilidad con las versiones anteriores: la compatibilidad con las versiones anteriores facilita la actualización del ADDF para incorporar las últimas características y actualizaciones de seguridad. Al cambiar el marco, impide la compatibilidad nativa con versiones anteriores de SeedFarmer, CodeSeeder y cualquier módulo principal del ADDF.
- Consecuencias de seguridad: cambiar el marco de implementación del ADDF es una tarea compleja que puede tener consecuencias de seguridad no deseadas. En el peor de los casos, los cambios en el marco pueden generar vulnerabilidades de seguridad.

Cuando sea posible, cree y personalice su propio código de módulo en lugar de modificar el marco de implementación del ADDF y el código del módulo principal del ADDF.

> **Note**
>
> Si considera que hay partes específicas del marco de implementación del ADDF que se deben mejorar o se debe reforzar aún más la seguridad, cuéntenos los cambios que realizaría en el repositorio del ADDF mediante una solicitud de cambios. Para obtener más información, consulte Contribuciones y revisiones de seguridad de código abierto.

Escritura de módulos personalizados en el ADDF

Crear un módulo de ADDF nuevo o ampliar un módulo existente es un concepto fundamental del ADDF. Al crear o personalizar módulos, le sugerimos que siga las prácticas recomendadas de seguridad de AWS generales y las prácticas recomendadas de su organización para una codificación segura. Además, le recomendamos que realice revisiones técnicas de seguridad internas o externas iniciales y periódicas, en función de los requisitos de seguridad de su organización, para reducir aún más el riesgo de problemas de seguridad.

Implementaciones del ADDF recurrentes

Implemente el ADDF y sus módulos tal y como se describe en la Guía de implementación del ADDF (GitHub). Para admitir las implementaciones del ADDF recurrentes que agregan, actualizan o eliminan recursos en sus cuentas de destino, SeedFarmer utiliza hashes MD5, almacenados en el Almacén de parámetros de su cadena de herramientas y cuentas de destino. Su fin es comparar la infraestructura que se encuentra implementada actualmente con la infraestructura definida en los archivos de manifiesto de su base de código local.

Este enfoque sigue el paradigma de GitOps, donde su repositorio de origen (la base de código local en la que opera SeedFarmer) es la fuente de información y la infraestructura declarada explícitamente en él es el resultado deseado de su implementación. Para obtener más información sobre GitOps, consulte ¿Qué es GitOps? (sitio web de GitLab).

Auditorías de seguridad recurrentes

Al igual que cualquier otro software de su organización, integre el ADDF y el código del módulo del ADDF personalizado en su ciclo de auditoría de seguridad, administración de riesgos de seguridad y revisión de seguridad.

Actualizaciones del ADDF

El ADDF recibe actualizaciones periódicas como parte de su continuo desarrollo. Esto incluye actualizaciones de características, así como mejoras y correcciones relacionadas con la seguridad. Le recomendamos que compruebe de forma periódica si hay nuevas versiones del marco y que implemente las actualizaciones de manera oportuna. Para obtener más información, consulte Pasos para actualizar el ADDF (documentación del ADDF).

Desactivación

Si el ADDF ya no es necesario, elimine el ADDF y todos los recursos relacionados de sus Cuentas de AWS. Cualquier infraestructura desactualizada o sin uso conlleva costos innecesarios y supone un riesgo potencial para la seguridad. Para obtener más información, consulte Pasos para destruir el ADDF (documentación del ADDF).

Pasos siguientes

En esta guía se analizan las prácticas recomendadas y consideraciones en materia de seguridad y operaciones a la hora de implementar el Marco de Datos de Conducción Autónoma (ADDF) en su entorno de Nube de AWS. En esta guía se analiza el modelo de responsabilidad compartida entre el usuario del ADDF, el equipo principal del ADDF y AWS para que comprenda su rol y sus responsabilidades a la hora de configurar y operar el ADDF de forma segura. También incluye recomendaciones a fin de operar el ADDF de forma segura durante todo su ciclo de vida, incluido recomendaciones específicas para el entorno.

Le recomendamos que se familiarice con los recursos en la sección de Recursos. Cuando se encuentre listo, podrá configurar el ADDF en función de las instrucciones de la Guía de implementación del ADDF (GitHub).

A medida que configure y utilice el ADDF, si considera que se debe mejorar el marco de implementación o reforzar aún más la seguridad, cuéntenos los cambios que realizaría en el repositorio del ADDF mediante una solicitud de cambios. Para obtener más información, consulte Contribuciones y revisiones de seguridad de código abierto.

Recursos

Documentación de AWS

- Desarrollar e implementar un flujo de trabajo personalizado mediante el ADDF en AWS (publicación de blog de AWS)
- Documentación del servicio de seguridad de AWS
- Security best practices in IAM (Prácticas recomendadas de seguridad en IAM)
- Administración y separación de cuentas de AWS
- Proceso de arranque para AWS CDK
- Modelo de responsabilidad compartida de AWS
- Marco de AWS Well-Architected

Recursos de código abierto

- Repositorio del ADDF (GitHub)
- Guía de implementación del ADDF (GitHub)
- Repositorio de CodeSeeder (GitHub)
- Repositorio de SeedFarmer (GitHub)

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. El presente documento: (a) tiene solo fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no supone ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, afirmaciones ni condiciones de ningún tipo, ya sean expresas o implícitas.

Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

© 2022 Amazon Web Services, Inc. o sus filiales. Todos los derechos reservados.

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quiere recibir notificaciones de futuras actualizaciones, puede suscribirse a las notificaciones RSS.

Cambio	Descripción	Fecha
Publicación inicial	—	15 de noviembre de 2022

AWS Glosario de orientación prescriptiva

Los siguientes son términos de uso común en las estrategias, guías y patrones proporcionados por AWS Prescriptive Guidance. Para sugerir entradas, utilice el enlace Enviar comentarios al final del glosario.

Números

Las 7 R

Siete estrategias de migración comunes para trasladar aplicaciones a la nube. Estas estrategias se basan en las 5 R que Gartner identificó en 2011 y consisten en lo siguiente:

- Refactorizar/rediseñar: traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: migre su base de datos Oracle local a la edición compatible con Postgre SQL de Amazon Aurora.
- Redefinir la plataforma (transportar y redefinir): traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Amazon Relational Database Service (RDSAmazon) para Oracle en el. Nube de AWS
- Recomprar (readquirir): cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: migre su sistema de gestión de relaciones con los clientes (CRM) a Salesforce.com.
- Volver a alojar (migrar mediante lift-and-shift): traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Oracle en una EC2 instancia del. Nube de AWS
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma local a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

- Retirar: retire o elimine las aplicaciones que ya no sean necesarias en un entorno de origen.

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas (mediante una herramienta de replicación bidireccional o mediante operaciones de escritura doble) y ambas bases de datos gestionan las transacciones de las aplicaciones conectadas durante la migración. Este método permite la migración en lotes pequeños y controlados, en lugar de requerir una transición única. Es más flexible, pero requiere más trabajo que la migración activa-pasiva.

migración activa-pasiva

Método de migración de bases de datos en el que las bases de datos de origen y destino se mantienen sincronizadas, pero solo la base de datos de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la base de datos de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

función agregada

SQLFunción que opera en un grupo de filas y calcula un único valor de retorno para el grupo. Entre los ejemplos de funciones agregadas se incluyen `SUM` y`MAX`.

IA

Véase inteligencia artificial.

AIOps

Consulte las operaciones de inteligencia artificial.

anonimización

El proceso de eliminar permanentemente la información personal de un conjunto de datos. La anonimización puede ayudar a proteger la privacidad personal. Los datos anonimizados ya no se consideran datos personales.

antipatrones

Una solución que se utiliza con frecuencia para un problema recurrente en el que la solución es contraproducente, ineficaz o menos eficaz que una alternativa.

control de aplicaciones

Un enfoque de seguridad que permite el uso únicamente de aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

cartera de aplicaciones

Recopilación de información detallada sobre cada aplicación que utiliza una organización, incluido el costo de creación y mantenimiento de la aplicación y su valor empresarial. Esta información es clave para el proceso de detección y análisis de la cartera y ayuda a identificar y priorizar las aplicaciones que se van a migrar, modernizar y optimizar.

inteligencia artificial (IA)

El campo de la informática que se dedica al uso de tecnologías informáticas para realizar funciones cognitivas que suelen estar asociadas a los seres humanos, como el aprendizaje, la resolución de problemas y el reconocimiento de patrones. Para más información, consulte ¿Qué es la inteligencia artificial?

operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo AIOps se utiliza en la estrategia de AWS migración, consulte la guía de integración de operaciones.

cifrado asimétrico

Algoritmo de cifrado que utiliza un par de claves, una clave pública para el cifrado y una clave privada para el descifrado. Puede compartir la clave pública porque no se utiliza para el descifrado, pero el acceso a la clave privada debe estar sumamente restringido.

atomicidad, consistencia, aislamiento, durabilidad () ACID

Conjunto de propiedades de software que garantizan la validez de los datos y la fiabilidad operativa de una base de datos, incluso en caso de errores, cortes de energía u otros problemas.

control de acceso basado en atributos () ABAC

La práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte ABACla AWS documentación de AWS Identity and Access Management (IAM).

origen de datos fidedigno

Ubicación en la que se almacena la versión principal de los datos, que se considera la fuente de información más fiable. Puede copiar los datos del origen de datos autorizado a otras ubicaciones con el fin de procesarlos o modificarlos, por ejemplo, anonimizarlos, redactarlos o seudonimizarlos.

Zona de disponibilidad

Una ubicación distinta dentro de una Región de AWS que está aislada de los fallos en otras zonas de disponibilidad y que proporciona una conectividad de red económica y de baja latencia con otras zonas de disponibilidad de la misma región.

AWS Marco de adopción de la nube ()AWS CAF

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAForganiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y la comunicación de las personas a fin de ayudar a la organización a prepararse para una adopción exitosa de la nube. Para obtener más información, consulte el AWS CAFsitio web y el AWS CAFdocumento técnico.

AWS Marco de calificación de la carga de trabajo ()AWS WQF

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQFse incluye con AWS

Schema Conversion Tool ()AWS SCT. Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

B

un bot malo

Un bot destinado a interrumpir o causar daño a personas u organizaciones.

BCP

Consulte la planificación de la continuidad del negocio.

gráfico de comportamiento

Una vista unificada e interactiva del comportamiento de los recursos y de las interacciones a lo largo del tiempo. Puede utilizar un gráfico de comportamiento con Amazon Detective para examinar los intentos de inicio de sesión fallidos, las API llamadas sospechosas y acciones similares. Para obtener más información, consulte Datos en un gráfico de comportamiento en la documentación de Detective.

sistema big-endian

Un sistema que almacena primero el byte más significativo. Véase también endianismo.

clasificación binaria

Un proceso que predice un resultado binario (una de las dos clases posibles). Por ejemplo, es posible que su modelo de ML necesite predecir problemas como “¿Este correo electrónico es spam o no es spam?” o “¿Este producto es un libro o un automóvil?”.

filtro de floración

Estructura de datos probabilística y eficiente en términos de memoria que se utiliza para comprobar si un elemento es miembro de un conjunto.

implementación azul/verde

Una estrategia de despliegue en la que se crean dos entornos separados pero idénticos. La versión actual de la aplicación se ejecuta en un entorno (azul) y la nueva versión de la aplicación en el otro entorno (verde). Esta estrategia le ayuda a revertirla rápidamente con un impacto mínimo.

bot

Aplicación de software que ejecuta tareas automatizadas a través de Internet y simula la actividad o interacción humana. Algunos bots son útiles o beneficiosos, como los rastreadores web que indexan información en Internet. Algunos otros bots, conocidos como bots malos, tienen como objetivo interrumpir o causar daños a personas u organizaciones.

botnet

Redes de bots que están infectadas por malware y que están bajo el control de una sola parte, conocida como pastor u operador de bots. Las botnets son el mecanismo más conocido para escalar los bots y su impacto.

rama

Área contenida de un repositorio de código. La primera rama que se crea en un repositorio es la rama principal. Puede crear una rama nueva a partir de una rama existente y, a continuación, desarrollar características o corregir errores en la rama nueva. Una rama que se genera para crear una característica se denomina comúnmente rama de característica. Cuando la característica se encuentra lista para su lanzamiento, se vuelve a combinar la rama de característica con la rama principal. Para obtener más información, consulte Acerca de las sucursales (GitHub documentación).

acceso con cristales rotos

En circunstancias excepcionales y mediante un proceso aprobado, un usuario puede acceder rápidamente a un sitio para el Cuenta de AWS que normalmente no tiene permisos de acceso. Para obtener más información, consulte el indicador Implemente procedimientos de rotura de cristales en la guía Well-Architected AWS .

estrategia de implementación sobre infraestructura existente

La infraestructura existente en su entorno. Al adoptar una estrategia de implementación sobre infraestructura existente para una arquitectura de sistemas, se diseña la arquitectura en función de las limitaciones de los sistemas y la infraestructura actuales. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

caché de búfer

El área de memoria donde se almacenan los datos a los que se accede con más frecuencia.

capacidad empresarial

Lo que hace una empresa para generar valor (por ejemplo, ventas, servicio al cliente o marketing). Las arquitecturas de microservicios y las decisiones de desarrollo pueden estar impulsadas por las capacidades empresariales. Para obtener más información, consulte la sección Organizado en torno a las capacidades empresariales del documento técnico Ejecutar microservicios en contenedores en AWS.

planificación de la continuidad del negocio () BCP

Plan que aborda el posible impacto de un evento disruptivo, como una migración a gran escala en las operaciones y permite a la empresa reanudar las operaciones rápidamente.

C

CAF

Consulte el marco AWS de adopción de la nube.

despliegue canario

El lanzamiento lento e incremental de una versión para los usuarios finales. Cuando está seguro, despliega la nueva versión y reemplaza la versión actual en su totalidad.

CCoE

Consulte Cloud Center of Excellence.

CDC

Consulte la captura de datos de cambios.

cambiar la captura de datos (CDC)

Proceso de seguimiento de los cambios en un origen de datos, como una tabla de base de datos, y registro de los metadatos relacionados con el cambio. Se puede utilizar CDC para varios fines, como auditar o replicar los cambios en un sistema de destino para mantener la sincronización.

ingeniería del caos

Introducir intencionalmente fallos o eventos disruptivos para poner a prueba la resiliencia de un sistema. Puedes usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estresen tus AWS cargas de trabajo y evalúen su respuesta.

CI/CD

Consulte la integración continua y la entrega continua.

clasificación

Un proceso de categorización que permite generar predicciones. Los modelos de ML para problemas de clasificación predicen un valor discreto. Los valores discretos siempre son distintos entre sí. Por ejemplo, es posible que un modelo necesite evaluar si hay o no un automóvil en una imagen.

cifrado del cliente

Cifrado de datos localmente, antes de que el objetivo los Servicio de AWS reciba.

Centro de excelencia en la nube (CCoE)

Equipo multidisciplinario que impulsa los esfuerzos de adopción de la nube en toda la organización, incluido el desarrollo de las prácticas recomendadas en la nube, la movilización de recursos, el establecimiento de plazos de migración y la dirección de la organización durante las transformaciones a gran escala. Para obtener más información, consulte las CCoEpublicaciones del blog de estrategia Nube de AWS empresarial.

computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar conectada a la tecnología de computación perimetral.

modelo operativo en la nube

En una organización de TI, el modelo operativo que se utiliza para crear, madurar y optimizar uno o más entornos de nube. Para obtener más información, consulte Creación de su modelo operativo de nube.

etapas de adopción de la nube

Las cuatro fases por las que suelen pasar las organizaciones cuando migran a Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir un CCoE modelo de operaciones)
- Migración: migración de aplicaciones individuales

- Reinvención: optimización de productos y servicios e innovación en la nube

Stephen Orban definió estas etapas en la entrada del blog The Journey Toward Cloud-First & the Stages of Adoption en el blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la guía de preparación para la migración.

CMDB

Consulte la base de datos de administración de la configuración.

repositorio de código

Una ubicación donde el código fuente y otros activos, como documentación, muestras y scripts, se almacenan y actualizan mediante procesos de control de versiones. Los repositorios en la nube más comunes incluyen GitHub o AWS CodeCommit. Cada versión del código se denomina rama. En una estructura de microservicios, cada repositorio se encuentra dedicado a una única funcionalidad. Una sola canalización de CI/CD puede utilizar varios repositorios.

caché en frío

Una caché de búfer que está vacía no está bien poblada o contiene datos obsoletos o irrelevantes. Esto afecta al rendimiento, ya que la instancia de la base de datos debe leer desde la memoria principal o el disco, lo que es más lento que leer desde la memoria caché del búfer.

datos fríos

Datos a los que se accede con poca frecuencia y que suelen ser históricos. Al consultar este tipo de datos, normalmente se aceptan consultas lentas. Trasladar estos datos a niveles o clases de almacenamiento de menor rendimiento y menos costosos puede reducir los costos.

visión artificial (CV)

Campo de la IA que utiliza el aprendizaje automático para analizar y extraer información de formatos visuales, como imágenes y vídeos digitales. Por ejemplo, AWS Panorama ofrece dispositivos que añaden CV a las redes de cámaras locales, y Amazon SageMaker proporciona algoritmos de procesamiento de imágenes para CV.

desviación de configuración

En el caso de una carga de trabajo, un cambio de configuración con respecto al estado esperado. Puede provocar que la carga de trabajo deje de cumplir las normas y, por lo general, es gradual e involuntario.

base de datos de administración de configuración () CMDB

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, se utilizan datos CMDB de una etapa de migración de descubrimiento y análisis de la cartera.

paquete de conformidad

Conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus comprobaciones de conformidad y seguridad. Puede implementar un paquete de conformidad como una entidad única en una Cuenta de AWS región o en una organización mediante una YAML plantilla. Para obtener más información, consulte los paquetes de conformidad en la AWS Config documentación.

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, presentación y producción del proceso de lanzamiento del software. La CI/CD se describe comúnmente como una canalización. La CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Consulte visión artificial.

D

datos en reposo

Datos que están estacionarios en la red, como los datos que se encuentran almacenados.

clasificación de datos

Un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de protección y retención adecuados para los datos. La clasificación de datos es un componente del pilar de seguridad del AWS Well-Architected Framework. Para obtener más información, consulte Clasificación de datos.

desviación de datos

Una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de machine learning, o un cambio significativo en los datos de entrada a lo largo del tiempo. La desviación de los datos puede reducir la calidad, la precisión y la imparcialidad generales de las predicciones de los modelos de machine learning.

datos en tránsito

Datos que se mueven de forma activa por la red, por ejemplo, entre los recursos de la red.

malla de datos

Un marco arquitectónico que proporciona una propiedad de datos distribuida y descentralizada con una administración y un gobierno centralizados.

minimización de datos

El principio de recopilar y procesar solo los datos estrictamente necesarios. Practicar la minimización de los datos Nube de AWS puede reducir los riesgos de privacidad, los costos y la huella de carbono de la analítica.

perímetro de datos

Un conjunto de barreras preventivas en su AWS entorno que ayudan a garantizar que solo las identidades confiables accedan a los recursos confiables desde las redes esperadas. Para obtener más información, consulte Crear un perímetro de datos sobre. AWS

preprocesamiento de datos

Transformar los datos sin procesar en un formato que su modelo de ML pueda analizar fácilmente. El preprocesamiento de datos puede implicar eliminar determinadas columnas o filas y corregir los valores faltantes, incoherentes o duplicados.

procedencia de los datos

El proceso de rastrear el origen y el historial de los datos a lo largo de su ciclo de vida, por ejemplo, la forma en que se generaron, transmitieron y almacenaron los datos.

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

Un sistema de administración de datos que respalde la inteligencia empresarial, como el análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para consultas y análisis.

lenguaje de definición de bases de datos (DDL)

Instrucciones o comandos para crear o modificar la estructura de tablas y objetos de una base de datos.

lenguaje de manipulación de bases de datos (DML)

Instrucciones o comandos para modificar (insertar, actualizar y eliminar) la información de una base de datos.

DDL

Consulte el lenguaje de definición de bases de datos.

conjunto profundo

Combinar varios modelos de aprendizaje profundo para la predicción. Puede utilizar conjuntos profundos para obtener una predicción más precisa o para estimar la incertidumbre de las predicciones.

aprendizaje profundo

Un subcampo del ML que utiliza múltiples capas de redes neuronales artificiales para identificar el mapeo entre los datos de entrada y las variables objetivo de interés.

defense-in-depth

Un enfoque de seguridad de la información en el que se distribuyen cuidadosamente una serie de mecanismos y controles de seguridad en una red informática para proteger la confidencialidad, la integridad y la disponibilidad de la red y de los datos que contiene. Al adoptar esta estrategia AWS, se añaden varios controles en diferentes capas de la AWS Organizations estructura para ayudar a proteger los recursos. Por ejemplo, un defense-in-depth enfoque podría combinar la autenticación multifactorial, la segmentación de la red y el cifrado.

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro para administrar las cuentas de la organización y gestionar los permisos de ese servicio. Esta

cuenta se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte Servicios que funcionan con AWS Organizations en la documentación de AWS Organizations .

Implementación

El proceso de hacer que una aplicación, características nuevas o correcciones de código se encuentren disponibles en el entorno de destino. La implementación abarca implementar cambios en una base de código y, a continuación, crear y ejecutar esa base en los entornos de la aplicación.

entorno de desarrollo

Consulte entorno.

control de detección

Un control de seguridad que se ha diseñado para detectar, registrar y alertar después de que se produzca un evento. Estos controles son una segunda línea de defensa, ya que lo advierten sobre los eventos de seguridad que han eludido los controles preventivos establecidos. Para obtener más información, consulte Controles de detección en Implementación de controles de seguridad en AWS.

mapeo del flujo de valor de desarrollo (DVSM)

Proceso que se utiliza para identificar y priorizar las restricciones que afectan negativamente a la velocidad y la calidad en el ciclo de vida del desarrollo de software. DVSMamplía el proceso de mapeo del flujo de valor diseñado originalmente para las prácticas de fabricación ajustada. Se centra en los pasos y los equipos necesarios para crear y transferir valor a través del proceso de desarrollo de software.

gemelo digital

Representación virtual de un sistema del mundo real, como un edificio, una fábrica, un equipo industrial o una línea de producción. Los gemelos digitales son compatibles con el mantenimiento predictivo, la supervisión remota y la optimización de la producción.

tabla de dimensiones

En un esquema en estrella, tabla más pequeña que contiene los atributos de datos sobre los datos cuantitativos de una tabla de hechos. Los atributos de la tabla de dimensiones suelen ser campos de texto o números discretos que se comportan como texto. Estos atributos se utilizan habitualmente para restringir consultas, filtrar y etiquetar conjuntos de resultados.

desastre

Un evento que impide que una carga de trabajo o un sistema cumplan sus objetivos empresariales en su ubicación principal de implementación. Estos eventos pueden ser desastres naturales, fallos técnicos o el resultado de acciones humanas, como una configuración incorrecta involuntaria o un ataque de malware.

recuperación de desastres (DR)

La estrategia y el proceso que se utilizan para minimizar el tiempo de inactividad y la pérdida de datos ocasionados por un desastre. Para obtener más información, consulte Recuperación ante desastres de cargas de trabajo en AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Consulte el lenguaje de manipulación de bases de datos.

diseño basado en el dominio

Un enfoque para desarrollar un sistema de software complejo mediante la conexión de sus componentes a dominios en evolución, o a los objetivos empresariales principales, a los que sirve cada componente. Este concepto lo introdujo Eric Evans en su libro, Diseño impulsado por el dominio: abordando la complejidad en el corazón del software (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte Modernizar la antigua Microsoft. ASP NET(ASMX) servicios web de forma incremental mediante contenedores y Amazon API Gateway.

DR

Consulte recuperación ante desastres.

detección de desviaciones

Seguimiento de las desviaciones con respecto a una configuración de referencia. Por ejemplo, puedes usarlo AWS CloudFormation para detectar desviaciones en los recursos del sistema o puedes usarlo AWS Control Tower para detectar cambios en tu landing zone que puedan afectar al cumplimiento de los requisitos de gobierno.

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

computación en la periferia

La tecnología que aumenta la potencia de cálculo de los dispositivos inteligentes en la periferia de una red de IoT. En comparación con la computación en nube, la computación perimetral puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

cifrado

Proceso informático que transforma datos de texto plano, legibles por humanos, en texto cifrado.

clave de cifrado

Cadena criptográfica de bits aleatorios que se genera mediante un algoritmo de cifrado. Las claves pueden variar en longitud y cada una se ha diseñado para ser impredecible y única.

endianidad

El orden en el que se almacenan los bytes en la memoria del ordenador. Los sistemas big-endianos almacenan primero el byte más significativo. Los sistemas Little-Endian almacenan primero el byte menos significativo.

punto de conexión

Consulte el punto final del servicio.

servicio de punto de conexión

Un servicio que puede alojar en una nube privada virtual (VPC) para compartirlo con otros usuarios. Puede crear un servicio de punto final con otros Cuentas de AWS o AWS Identity and Access Management (IAM) principales AWS PrivateLink y conceder permisos a ellos. Estas cuentas o entidades principales pueden conectarse a su servicio de puntos finales de forma privada mediante la creación de puntos finales de interfazVPC. Para obtener más información, consulte Crear un servicio de punto final en la documentación de Amazon Virtual Private Cloud (AmazonVPC).

planificación de recursos empresariales (ERP)

Un sistema que automatiza y gestiona los procesos empresariales clave (como la contabilidad y la gestión de proyectos) de una empresa. MES

cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte Cifrado de sobres en la documentación de AWS Key Management Service (AWS KMS).

environment

Una instancia de una aplicación en ejecución. Los siguientes son los tipos de entornos más comunes en la computación en la nube:

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.
- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En una canalización de CI/CD, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, los aspectos más importantes de la AWS CAF seguridad incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la Guía de implementación del programa.

ERP

Consulte la planificación de recursos empresariales.

análisis exploratorio de datos () EDA

El proceso de analizar un conjunto de datos para comprender sus características principales. Se recopilan o agregan datos y, a continuación, se realizan las investigaciones iniciales para

encontrar patrones, detectar anomalías y comprobar las suposiciones. EDAse realiza mediante el cálculo de estadísticas resumidas y la creación de visualizaciones de datos.

F

tabla de datos

La tabla central de un esquema en forma de estrella. Almacena datos cuantitativos sobre las operaciones comerciales. Normalmente, una tabla de hechos contiene dos tipos de columnas: las que contienen medidas y las que contienen una clave externa para una tabla de dimensiones.

fallan rápidamente

Una filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de un enfoque ágil.

límite de aislamiento de fallas

En el Nube de AWS, un límite, como una zona de disponibilidad Región de AWS, un plano de control o un plano de datos, que limita el efecto de una falla y ayuda a mejorar la resiliencia de las cargas de trabajo. Para obtener más información, consulte Límites de AWS aislamiento de errores.

rama de característica

Consulte la sucursal.

características

Los datos de entrada que se utilizan para hacer una predicción. Por ejemplo, en un contexto de fabricación, las características pueden ser imágenes que se capturan periódicamente desde la línea de fabricación.

importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, se expresa como una puntuación numérica que se puede calcular mediante diversas técnicas, como las explicaciones aditivas de Shapley (SHAP) y los gradientes integrados. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con:.AWS

transformación de funciones

Optimizar los datos para el proceso de ML, lo que incluye enriquecer los datos con fuentes adicionales, escalar los valores o extraer varios conjuntos de información de un solo campo de

datos. Esto permite que el modelo de ML se beneficie de los datos. Por ejemplo, si divide la fecha del “27 de mayo de 2021 00:15:37” en “jueves”, “mayo”, “2021” y “15”, puede ayudar al algoritmo de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

FGAC

Consulte control de acceso detallado.

control de acceso detallado () FGAC

El uso de varias condiciones que tienen por objetivo permitir o denegar una solicitud de acceso.

migración relámpago

Método de migración de bases de datos que utiliza la replicación continua de datos mediante la captura de datos modificados para migrar los datos en el menor tiempo posible, en lugar de utilizar un enfoque gradual. El objetivo es reducir al mínimo el tiempo de inactividad.

G

bloqueo geográfico

Consulta las restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

En Amazon CloudFront, una opción para impedir que los usuarios de países específicos accedan a las distribuciones de contenido. Puede utilizar una lista de permitidos o bloqueados para especificar los países aprobados y prohibidos. Para obtener más información, consulta Restringir la distribución geográfica del contenido en la CloudFront documentación.

Flujo de trabajo de Gitflow

Un enfoque en el que los entornos inferiores y superiores utilizan diferentes ramas en un repositorio de código fuente. El flujo de trabajo de Gitflow se considera heredado, y el flujo de trabajo basado en enlaces troncales es el enfoque moderno preferido.

estrategia de implementación desde cero

La ausencia de infraestructura existente en un entorno nuevo. Al adoptar una estrategia de implementación desde cero para una arquitectura de sistemas, puede seleccionar todas las

tecnologías nuevas sin que estas deban ser compatibles con una infraestructura existente, lo que también se conoce como implementación sobre infraestructura existente. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y el cumplimiento en todas las unidades organizativas (). OUs Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de IAM permisos. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

JA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que utilice un motor de base de datos diferente (por ejemplo, de Oracle a Amazon Aurora). La migración heterogénea suele ser parte de un esfuerzo de rediseño de la arquitectura y convertir el esquema puede ser una tarea compleja. AWS ofrece AWS SCT, lo cual ayuda con las conversiones de esquemas.

alta disponibilidad (HA)

La capacidad de una carga de trabajo para funcionar de forma continua, sin intervención, en caso de desafíos o desastres. Los sistemas de alta disponibilidad están diseñados para realizar una conmutación por error automática, ofrecer un rendimiento de alta calidad de forma constante y gestionar diferentes cargas y fallos con un impacto mínimo en el rendimiento.

modernización histórica

Un enfoque utilizado para modernizar y actualizar los sistemas de tecnología operativa (TO) a fin de satisfacer mejor las necesidades de la industria manufacturera. Un histórico es un tipo de base de datos que se utiliza para recopilar y almacenar datos de diversas fuentes en una fábrica.

migración homogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que comparte el mismo motor de base de datos (por ejemplo, Microsoft SQL Server a Amazon RDS for SQL Server). La migración homogénea suele formar parte de un esfuerzo para volver a alojar o redefinir la plataforma. Puede utilizar las utilidades de bases de datos nativas para migrar el esquema.

datos recientes

Datos a los que se accede con frecuencia, como datos en tiempo real o datos traslacionales recientes. Por lo general, estos datos requieren un nivel o una clase de almacenamiento de alto rendimiento para proporcionar respuestas rápidas a las consultas.

hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, una revisión se suele realizar fuera del flujo de trabajo de DevOps publicación habitual.

periodo de hiperatención

Periodo, inmediatamente después de la transición, durante el cual un equipo de migración administra y monitorea las aplicaciones migradas en la nube para solucionar cualquier problema. Por lo general, este periodo dura de 1 a 4 días. Al final del periodo de hiperatención, el equipo de migración suele transferir la responsabilidad de las aplicaciones al equipo de operaciones en la nube.

I

IaC

Vea la infraestructura como código.

políticas basadas en identidad

Política asociada a uno o más IAM directores que define sus permisos en el Nube de AWS entorno.

aplicación inactiva

Aplicación que tiene un uso medio CPU de memoria entre el 5 y el 20 por ciento durante un período de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

Un modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar, aplicar parches o modificar la infraestructura existente. Las infraestructuras inmutables son intrínsecamente más consistentes, fiables y predecibles que las infraestructuras mutables. Para obtener más información, consulte las prácticas recomendadas para implementar con una infraestructura inmutable en Well-Architected Framework AWS .

entrante (ingreso) VPC

En una arquitectura AWS multicuenta, VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

migración gradual

Estrategia de transición en la que se migra la aplicación en partes pequeñas en lugar de realizar una transición única y completa. Por ejemplo, puede trasladar inicialmente solo unos pocos microservicios o usuarios al nuevo sistema. Tras comprobar que todo funciona correctamente, puede trasladar microservicios o usuarios adicionales de forma gradual hasta que pueda retirar su sistema heredado. Esta estrategia reduce los riesgos asociados a las grandes migraciones.

Industria 4.0

Un término que Klaus Schwab introdujo en 2016 para referirse a la modernización de los procesos de fabricación mediante avances en la conectividad, los datos en tiempo real, la automatización, el análisis y la inteligencia artificial/aprendizaje automático.

infraestructura

Todos los recursos y activos que se encuentran en el entorno de una aplicación.

infraestructura como código (IaC)

Proceso de aprovisionamiento y administración de la infraestructura de una aplicación mediante un conjunto de archivos de configuración. La IaC se ha diseñado para ayudarlo a centralizar la administración de la infraestructura, estandarizar los recursos y escalar con rapidez a fin de que los entornos nuevos sean repetibles, fiables y consistentes.

Internet de las cosas industrial () IIoT

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la agricultura. Para obtener más información, consulte Creación de una estrategia de transformación digital del Internet de las cosas (IIoT) industrial.

inspección VPC

En una arquitectura de AWS múltiples cuentas, una arquitectura centralizada VPC que gestiona las inspecciones del tráfico de red entre Internet y las redes locales VPCs (en una misma o diferente Regiones de AWS). La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entrada, salida e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

Internet de las cosas (IoT)

Red de objetos físicos conectados con sensores o procesadores integrados que se comunican con otros dispositivos y sistemas a través de Internet o de una red de comunicación local. Para obtener más información, consulte ¿Qué es IoT?.

interpretabilidad

Característica de un modelo de machine learning que describe el grado en que un ser humano puede entender cómo las predicciones del modelo dependen de sus entradas. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con. AWS

IoT

Consulte Internet de las cosas.

Biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. ITILproporciona la base paraITSM.

Administración de servicios de TI (ITSM)

Actividades asociadas con el diseño, la implementación, la administración y el soporte de los servicios de TI para una organización. Para obtener información sobre la integración de las operaciones en la nube con ITSM las herramientas, consulte la guía de integración de operaciones.

ITIL

Consulte la biblioteca de información de TI.

ITSM

Consulte Administración de servicios de TI.

L

control de acceso basado en etiquetas () LBAC

Una implementación del control de acceso obligatorio (MAC) en la que a los usuarios y a los propios datos se les asigna explícitamente un valor de etiqueta de seguridad. La intersección entre la etiqueta de seguridad del usuario y la etiqueta de seguridad de los datos determina qué filas y columnas puede ver el usuario.

zona de aterrizaje

Una landing zone es un AWS entorno multicuenta bien diseñado, escalable y seguro. Este es un punto de partida desde el cual las empresas pueden lanzar e implementar rápidamente cargas de trabajo y aplicaciones con confianza en su entorno de seguridad e infraestructura. Para obtener más información sobre las zonas de aterrizaje, consulte Configuración de un entorno de AWS seguro y escalable con varias cuentas.

migración grande

Migración de 300 servidores o más.

LBAC

Consulte el control de acceso basado en etiquetas.

privilegio mínimo

La práctica recomendada de seguridad que consiste en conceder los permisos mínimos necesarios para realizar una tarea. Para obtener más información, consulte Aplicar permisos con privilegios mínimos en la documentación. IAM

migrar mediante lift-and-shift

Consulte 7 Rs.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Véase también endianness.

entornos inferiores

Véase entorno.

M

machine learning (ML)

Un tipo de inteligencia artificial que utiliza algoritmos y técnicas para el reconocimiento y el aprendizaje de patrones. El ML analiza y aprende de los datos registrados, como los datos del Internet de las cosas (IoT), para generar un modelo estadístico basado en patrones. Para más información, consulte Machine learning.

rama principal

Ver sucursal.

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware puede interrumpir los sistemas informáticos, filtrar información confidencial u obtener acceso no autorizado. Algunos ejemplos de malware son los virus, los gusanos, el ransomware, los troyanos, el spyware y los keyloggers.

servicios gestionados

Servicios de AWS para los que AWS opera la capa de infraestructura, el sistema operativo y las plataformas, y usted accede a los puntos finales para almacenar y recuperar datos. Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB son ejemplos de servicios gestionados. También se conocen como servicios abstractos.

sistema de ejecución de fabricación () MES

Un sistema de software para rastrear, monitorear, documentar y controlar los procesos de producción que convierten las materias primas en productos terminados en el taller.

MAP

Consulte Migration Acceleration Program.

mecanismo

Un proceso completo en el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para realizar ajustes. Un mecanismo es un ciclo que se refuerza y mejora a sí mismo a medida que funciona. Para obtener más información, consulte Creación de mecanismos en el AWS Well-Architected Framework.

cuenta de miembro

Todas las Cuentas de AWS demás cuentas, excepto la de administración, que forman parte de una organización. AWS Organizations Una cuenta no puede pertenecer a más de una organización a la vez.

MES

Consulte el sistema de ejecución de la fabricación.

Transporte de telemetría y cola de mensajes () MQTT

Un protocolo de comunicación ligero machine-to-machine (M2M), basado en el patrón de publicación/suscripción, para dispositivos de IoT con recursos limitados.

microservicio

Un servicio pequeño e independiente que se comunica a través de una red bien definida APIs y que, por lo general, es propiedad de equipos pequeños e independientes. Por ejemplo, un sistema de seguros puede incluir microservicios que se adapten a las capacidades empresariales, como las de ventas o marketing, o a subdominios, como las de compras, reclamaciones o análisis. Los beneficios de los microservicios incluyen la agilidad, la escalabilidad flexible, la facilidad de implementación, el código reutilizable y la resiliencia. Para obtener más información, consulte Integrar microservicios mediante AWS servicios sin servidor.

arquitectura de microservicios

Un enfoque para crear una aplicación con componentes independientes que ejecutan cada proceso de la aplicación como un microservicio. Estos microservicios se comunican a través de una interfaz bien definida mediante un uso ligero. APIs Cada microservicio de esta arquitectura se puede actualizar, implementar y escalar para satisfacer la demanda de funciones específicas de una aplicación. Para obtener más información, consulte Implementación de microservicios en. AWS

Migration Acceleration Program (MAP)

Un AWS programa que brinda soporte de consultoría, capacitación y servicios para ayudar a las organizaciones a construir una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. MAPincluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración habituales.

migración a escala

Proceso de transferencia de la mayoría de la cartera de aplicaciones a la nube en oleadas, con más aplicaciones desplazadas a un ritmo más rápido en cada oleada. En esta fase, se utilizan las prácticas recomendadas y las lecciones aprendidas en las fases anteriores para implementar una fábrica de migración de equipos, herramientas y procesos con el fin de agilizar la migración de las cargas de trabajo mediante la automatización y la entrega ágil. Esta es la tercera fase de la estrategia de migración de AWS.

fábrica de migración

Equipos multifuncionales que agilizan la migración de las cargas de trabajo mediante enfoques automatizados y ágiles. Los equipos de las fábricas de migración suelen estar compuestos por analistas y propietarios de operaciones, ingenieros de migración, desarrolladores y DevOps profesionales que trabajan a pasos agigantados. Entre el 20 y el 50 por ciento de la cartera de aplicaciones empresariales se compone de patrones repetidos que pueden optimizarse mediante un enfoque de fábrica. Para obtener más información, consulte la discusión sobre las fábricas de migración y la Guía de fábricas de migración a la nube en este contenido.

metadatos de migración

Información sobre la aplicación y el servidor que se necesita para completar la migración. Cada patrón de migración requiere un conjunto diferente de metadatos de migración. Algunos ejemplos de metadatos de migración son la subred de destino, el grupo de seguridad y AWS la cuenta.

patrón de migración

Tarea de migración repetible que detalla la estrategia de migración, el destino de la migración y la aplicación o el servicio de migración utilizados. Ejemplo: realoje la migración a Amazon EC2 con AWS Application Migration Service.

Evaluación de la cartera de migración () MPA

Una herramienta en línea que proporciona información para validar el argumento empresarial para migrar a. Nube de AWS MPAproporciona una evaluación detallada de la cartera (tamaño

correcto de los servidores, precios, TCO comparaciones y análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de la oleada). La MPAherramienta (requiere iniciar sesión) está disponible de forma gratuita para todos los consultores y AWS consultores de los socios. APN

Evaluación de la preparación para la migración (MRA)

El proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar los puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas, utilizando la AWS CAF. Para obtener más información, consulte la Guía de preparación para la migración. MRAes la primera fase de la estrategia de AWS migración.

estrategia de migración

El enfoque utilizado para migrar una carga de trabajo a Nube de AWS. Para obtener más información, consulte la entrada de las 7 R de este glosario y consulte Movilice a su organización para acelerar las migraciones a gran escala.

ML

Consulte el aprendizaje automático.

modernización

Transformar una aplicación obsoleta (antigua o monolítica) y su infraestructura en un sistema ágil, elástico y de alta disponibilidad en la nube para reducir los gastos, aumentar la eficiencia y aprovechar las innovaciones. Para obtener más información, consulte Estrategia para modernizar las aplicaciones en el Nube de AWS.

evaluación de la preparación para la modernización

Evaluación que ayuda a determinar la preparación para la modernización de las aplicaciones de una organización; identifica los beneficios, los riesgos y las dependencias; y determina qué tan bien la organización puede soportar el estado futuro de esas aplicaciones. El resultado de la evaluación es un esquema de la arquitectura objetivo, una hoja de ruta que detalla las fases de desarrollo y los hitos del proceso de modernización y un plan de acción para abordar las brechas identificadas. Para obtener más información, consulte Evaluación de la preparación para la modernización de las aplicaciones en el Nube de AWS.

aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar una arquitectura de microservicios. Para obtener más información, consulte Descomposición de monolitos en microservicios.

MPA

Consulte Evaluación de la cartera de migración.

MQTT

Consulte Message Queue Queue Telemetría y Transporte.

clasificación multiclase

Un proceso que ayuda a generar predicciones para varias clases (predice uno de más de dos resultados). Por ejemplo, un modelo de ML podría preguntar “¿Este producto es un libro, un automóvil o un teléfono?” o “¿Qué categoría de productos es más interesante para este cliente?”.

infraestructura mutable

Un modelo que actualiza y modifica la infraestructura existente para las cargas de trabajo de producción. Para mejorar la coherencia, la fiabilidad y la previsibilidad, el AWS Well-Architected Framework recomienda el uso de una infraestructura inmutable como práctica recomendada.

O

OAC

Consulte el control de acceso de origen.

OAI

Consulte la identidad de acceso de origen.

OCM

Consulte gestión del cambio organizacional.

migración fuera de línea

Método de migración en el que la carga de trabajo de origen se elimina durante el proceso de migración. Este método implica un tiempo de inactividad prolongado y, por lo general, se utiliza para cargas de trabajo pequeñas y no críticas.

OI

Consulte integración de operaciones.

OLA

Consulte el acuerdo a nivel operativo.

migración en línea

Método de migración en el que la carga de trabajo de origen se copia al sistema de destino sin que se desconecte. Las aplicaciones que están conectadas a la carga de trabajo pueden seguir funcionando durante la migración. Este método implica un tiempo de inactividad nulo o mínimo y, por lo general, se utiliza para cargas de trabajo de producción críticas.

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

Comunicaciones de proceso abierto: arquitectura unificada (OPC-UA)

Un protocolo de comunicación machine-to-machine (M2M) para la automatización industrial. OPC-UA proporciona un estándar de interoperabilidad con esquemas de cifrado, autenticación y autorización de datos.

acuerdo a nivel operativo () OLA

Un acuerdo que aclara lo que los grupos de TI funcionales se prometen ofrecer entre sí, para respaldar un acuerdo de nivel de servicio (). SLA

revisión de la preparación operativa () ORR

Una lista de preguntas y las mejores prácticas asociadas que le ayudan a comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles fallos. Para obtener más información, consulte Operational Readiness Reviews (ORR) en AWS Well-Architected Framework.

tecnología operativa (OT)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En la industria manufacturera, la

integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de la industria 4.0.

integración de operaciones (OI)

Proceso de modernización de las operaciones en la nube, que implica la planificación de la preparación, la automatización y la integración. Para obtener más información, consulte la Guía de integración de las operaciones.

registro de seguimiento organizativo

Un registro creado por el AWS CloudTrail que se registran todos los eventos para todos Cuentas de AWS los miembros de una organización AWS Organizations. Este registro de seguimiento se crea en cada Cuenta de AWS que forma parte de la organización y realiza un seguimiento de la actividad en cada cuenta. Para obtener más información, consulte Crear un registro para una organización en la CloudTrail documentación.

gestión del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. OCMayuda a las organizaciones a prepararse para los nuevos sistemas y estrategias y a realizar la transición a ellos acelerando la adopción del cambio, abordando los problemas de la transición e impulsando los cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración de las personas, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la OCMguía.

control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso y proteger el contenido del Amazon Simple Storage Service (Amazon S3). OACadmite todos los depósitos de S3 Regiones de AWS, el cifrado del lado del servidor con AWS KMS (SSE-KMS) y el cifrado dinámico `PUT` y `DELETE` las solicitudes al depósito de S3.

identidad de acceso de origen () OAI

En CloudFront, una opción para restringir el acceso y proteger el contenido de Amazon S3. Cuando lo usaOAI, CloudFront crea un principal con el que Amazon S3 puede autenticarse. Los directores autenticados solo pueden acceder al contenido de un bucket de S3 a través de una distribución específica. CloudFront Consulte también OAC, que proporciona un control de acceso mejorado y más detallado.

ORR

Consulte la revisión de la preparación operativa.

NO

Consulte tecnología operativa.

saliente (salida) VPC

En una arquitectura AWS multicuenta, VPC que gestiona las conexiones de red que se inician desde una aplicación. La arquitectura de referencia de AWS seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

P

límite de permisos

Una política IAM de administración asociada a IAM los directores para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte los límites de los permisos en la IAM documentación.

información de identificación personal (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos PII incluyen nombres, direcciones e información de contacto.

PII

Consulte la información de identificación personal.

manual de estrategias

Conjunto de pasos predefinidos que capturan el trabajo asociado a las migraciones, como la entrega de las funciones de operaciones principales en la nube. Un manual puede adoptar la forma de scripts, manuales de procedimientos automatizados o resúmenes de los procesos o pasos necesarios para operar un entorno modernizado.

PLC

Consulte controlador lógico programable.

PLM

Consulte la gestión del ciclo de vida del producto.

política

Un objeto que puede definir los permisos (consulte la política basada en la identidad), especifique las condiciones de acceso (consulte la política basada en los recursos) o defina los permisos máximos para todas las cuentas de una organización AWS Organizations (consulte la política de control de servicios).

persistencia políglota

Elegir de forma independiente la tecnología de almacenamiento de datos de un microservicio en función de los patrones de acceso a los datos y otros requisitos. Si sus microservicios tienen la misma tecnología de almacenamiento de datos, pueden enfrentarse a desafíos de implementación o experimentar un rendimiento deficiente. Los microservicios se implementan más fácilmente y logran un mejor rendimiento y escalabilidad si utilizan el almacén de datos que mejor se adapte a sus necesidades. Para obtener más información, consulte Habilitación de la persistencia de datos en los microservicios.

evaluación de cartera

Proceso de detección, análisis y priorización de la cartera de aplicaciones para planificar la migración. Para obtener más información, consulte la Evaluación de la preparación para la migración.

predicate

Una condición de consulta que devuelve `true` o `false`, normalmente, se encuentra en una cláusula `WHERE`.

pulsar un predicado

Técnica de optimización de consultas de bases de datos que filtra los datos de la consulta antes de transferirlos. Esto reduce la cantidad de datos que se deben recuperar y procesar de la base de datos relacional y mejora el rendimiento de las consultas.

control preventivo

Un control de seguridad diseñado para evitar que ocurra un evento. Estos controles son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Para obtener más información, consulte Controles preventivos en Implementación de controles de seguridad en AWS.

entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz de un Cuenta de AWS, un IAM rol o un usuario. Para obtener más información, consulte los términos y conceptos de Principal in Roles en la IAM documentación.

Privacidad desde el diseño

Un enfoque de ingeniería de sistemas que tiene en cuenta la privacidad durante todo el proceso de ingeniería.

zonas alojadas privadas

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a DNS las consultas de un dominio y sus subdominios dentro de uno o másVPCs. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

Un control de seguridad diseñado para evitar el despliegue de recursos no conformes. Estos controles escanean los recursos antes de aprovisionarlos. Si el recurso no cumple con el control, significa que no está aprovisionado. Para obtener más información, consulte la guía de referencia de controles en la AWS Control Tower documentación y consulte Controles proactivos en Implementación de controles de seguridad en AWS.

gestión del ciclo de vida del producto (PLM)

La gestión de los datos y los procesos de un producto a lo largo de todo su ciclo de vida, desde el diseño, el desarrollo y el lanzamiento, pasando por el crecimiento y la madurez, hasta el rechazo y la retirada.

entorno de producción

Consulte el entorno.

controlador lógico programable () PLC

En la industria manufacturera, una computadora adaptable y altamente confiable que monitorea las máquinas y automatiza los procesos de fabricación.

seudonimización

El proceso de reemplazar los identificadores personales de un conjunto de datos por valores de marcadores de posición. La seudonimización puede ayudar a proteger la privacidad personal. Los datos seudonimizados siguen considerándose datos personales.

publicar/suscribirse (pub/sub)

Un patrón que permite las comunicaciones asíncronas entre microservicios para mejorar la escalabilidad y la capacidad de respuesta. Por ejemplo, en un microservicio basado en microservicios MES, un microservicio puede publicar mensajes de eventos en un canal al que se puedan suscribir otros microservicios. El sistema puede añadir nuevos microservicios sin cambiar el servicio de publicación.

Q

plan de consulta

Serie de pasos, como instrucciones, que se utilizan para acceder a los datos de un sistema de base de datos SQL relacional.

regresión del plan de consulta

El optimizador de servicios de la base de datos elige un plan menos óptimo que antes de un cambio determinado en el entorno de la base de datos. Los cambios en estadísticas, restricciones, configuración del entorno, enlaces de parámetros de consultas y actualizaciones del motor de base de datos PostgreSQL pueden provocar una regresión del plan.

R

RACImatriz

Véase responsable, responsable, consultado, informado (RACI).

ransomware

Software malicioso que se ha diseñado para bloquear el acceso a un sistema informático o a los datos hasta que se efectúe un pago.

RASCImatriz

Véase responsable, responsable, consultado, informado (RACI).

RCAC

Consulte el control de acceso por filas y columnas.

read replica

Una copia de una base de datos que se utiliza con fines de solo lectura. Puede enrutar las consultas a la réplica de lectura para reducir la carga en la base de datos principal.

rediseñar

Ver 7 Rs.

objetivo de punto de recuperación (RPO)

La cantidad de tiempo máximo aceptable desde el último punto de recuperación de datos. Esto determina qué se considera una pérdida de datos aceptable entre el último punto de recuperación y la interrupción del servicio.

objetivo de tiempo de recuperación (RTO)

La demora máxima aceptable entre la interrupción del servicio y el restablecimiento del servicio.

refactorizar

Ver 7 Rs.

Región

Una colección de AWS recursos en un área geográfica. Cada uno Región de AWS está aislado e independiente de los demás para proporcionar tolerancia a las fallas, estabilidad y resiliencia. Para obtener más información, consulte Regiones de AWS Especificar qué cuenta puede usar.

regresión

Una técnica de ML que predice un valor numérico. Por ejemplo, para resolver el problema de “¿A qué precio se venderá esta casa?”, un modelo de ML podría utilizar un modelo de regresión lineal para predecir el precio de venta de una vivienda en función de datos conocidos sobre ella (por ejemplo, los metros cuadrados).

volver a alojar

Consulte 7 Rs.

versión

En un proceso de implementación, el acto de promover cambios en un entorno de producción.

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

resilencia

La capacidad de una aplicación para resistir las interrupciones o recuperarse de ellas. La alta disponibilidad y la recuperación ante desastres son consideraciones comunes a la hora de planificar la resiliencia en el. Nube de AWS Para obtener más información, consulte Nube de AWS Resiliencia.

política basada en recursos

Una política asociada a un recurso, como un bucket de Amazon S3, un punto de conexión o una clave de cifrado. Este tipo de política especifica a qué entidades principales se les permite el acceso, las acciones compatibles y cualquier otra condición que deba cumplirse.

matriz responsable, responsable, consultada, informada (RACI)

Una matriz que define las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones de la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), contable (A), consultado (C) e informado (I). El tipo de soporte (S) es opcional. Si incluye el soporte, la matriz se denomina RASCImatriz y, si la excluye, se denomina RACImatriz.

control receptivo

Un control de seguridad que se ha diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Para obtener más información, consulte Controles receptivos en Implementación de controles de seguridad en AWS.

retain

Consulte 7 Rs.

jubilarse

Ver 7 Rs.

rotación

Proceso de actualizar periódicamente un secreto para dificultar el acceso de un atacante a las credenciales.

control de acceso por filas y columnas (RCAC)

El uso de SQL expresiones básicas y flexibles que tienen reglas de acceso definidas. RCACconsta de permisos de fila y máscaras de columnas.

RPO

Consulte el objetivo del punto de recuperación.

RTO

Consulte el objetivo de tiempo de recuperación.

manual de procedimientos

Conjunto de procedimientos manuales o automatizados necesarios para realizar una tarea específica. Por lo general, se diseñan para agilizar las operaciones o los procedimientos repetitivos con altas tasas de error.

S

SAML2.0

Un estándar abierto que utilizan muchos proveedores de identidad (IdPs). Esta función permite el inicio de sesión único (SSO) federado, de modo que los usuarios pueden iniciar sesión AWS Management Console o llamar a las AWS API operaciones sin tener que crear un registro de usuario IAM para todos los miembros de la organización. Para obtener más información sobre la federación SAML basada en 2.0, consulte Acerca de la federación basada SAML en 2.0 en la documentación. IAM

SCADA

Consulte el control de supervisión y la adquisición de datos.

SCP

Consulte la política de control de servicios.

secreta

Información confidencial o restringida, como una contraseña o credenciales de usuario, que almacene de forma cifrada. AWS Secrets Manager Se compone del valor secreto y sus

metadatos. El valor secreto puede ser binario, una sola cadena o varias cadenas. Para obtener más información, consulta ¿Qué hay en un secreto de Secrets Manager? en la documentación de Secrets Manager.

control de seguridad

Barrera de protección técnica o administrativa que impide, detecta o reduce la capacidad de un agente de amenazas para aprovechar una vulnerabilidad de seguridad. Hay cuatro tipos principales de controles de seguridad: preventivos, de detección, de respuesta y proactivos.

refuerzo de la seguridad

Proceso de reducir la superficie expuesta a ataques para hacerla más resistente a los ataques. Esto puede incluir acciones, como la eliminación de los recursos que ya no se necesitan, la implementación de prácticas recomendadas de seguridad consistente en conceder privilegios mínimos o la desactivación de características innecesarias en los archivos de configuración.

sistema de información de seguridad y gestión de eventos (SIEM)

Herramientas y servicios que combinan los sistemas de gestión de la información de seguridad (SIM) y de gestión de eventos de seguridad (SEM). Un SIEM sistema recopila, monitorea y analiza datos de servidores, redes, dispositivos y otras fuentes para detectar amenazas y brechas de seguridad y generar alertas.

automatización de las respuestas de seguridad

Una acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o remediarlo. Estas automatizaciones sirven como controles de seguridad detectables o adaptables que le ayudan a implementar las mejores prácticas AWS de seguridad. Algunos ejemplos de acciones de respuesta automática incluyen la modificación de un grupo VPC de seguridad, la aplicación de parches a una EC2 instancia de Amazon o la rotación de credenciales.

cifrado del servidor

Cifrado de los datos en su destino, por parte de Servicio de AWS quien los recibe.

política de control de servicios (SCP)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPsdefina barreras o establezca límites a las acciones que un administrador puede delegar en usuarios o roles. Puede utilizarlas SCPs como listas de permitidos o rechazados para especificar qué servicios o acciones están permitidos o

prohibidos. Para obtener más información, consulte las políticas de control de servicios en la AWS Organizations documentación.

punto de enlace de servicio

El URL del punto de entrada de un Servicio de AWS. Para conectarse mediante programación a un servicio de destino, puede utilizar un punto de conexión. Para obtener más información, consulte Puntos de conexión de Servicio de AWS en Referencia general de AWS.

acuerdo de nivel de servicio () SLA

Acuerdo que aclara lo que un equipo de TI se compromete a ofrecer a los clientes, como el tiempo de actividad y el rendimiento del servicio.

indicador de nivel de servicio () SLI

Medición de un aspecto del rendimiento de un servicio, como la tasa de errores, la disponibilidad o el rendimiento.

objetivo de nivel de servicio () SLO

Una métrica objetivo que representa el estado de un servicio, medido mediante un indicador de nivel de servicio.

modelo de responsabilidad compartida

Un modelo que describe la responsabilidad que compartes con respecto a la seguridad y AWS el cumplimiento de la nube. AWS es responsable de la seguridad de la nube, mientras que usted es responsable de la seguridad en la nube. Para obtener más información, consulte el Modelo de responsabilidad compartida.

SIEM

Consulte la información de seguridad y el sistema de gestión de eventos.

punto único de fallo (SPOF)

Una falla en un único componente crítico de una aplicación que puede interrumpir el sistema.

SLA

Consulte el acuerdo de nivel de servicio.

SLI

Consulte el indicador de nivel de servicio.

SLO

Consulte el objetivo de nivel de servicio.

split-and-seed modelo

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para obtener más información, consulte Enfoque gradual para modernizar las aplicaciones en el. Nube de AWS

SPOF

Consulte el punto único de fallo.

esquema en forma de estrella

Estructura organizativa de una base de datos que utiliza una tabla de datos grande para almacenar datos transaccionales o medidos y una o más tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para usarse en un almacén de datos o con fines de inteligencia empresarial.

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda desmantelar el sistema heredado. Este patrón utiliza la analogía de una higuera que crece hasta convertirse en un árbol estable y, finalmente, se apodera y reemplaza a su host. El patrón fue presentado por Martin Fowler como una forma de gestionar el riesgo al reescribir sistemas monolíticos. Para ver un ejemplo de cómo aplicar este patrón, consulta Modernizar la versión antigua de MicrosoftASP. NET(ASMX) servicios web de forma incremental mediante contenedores y Amazon API Gateway.

subred

Un rango de direcciones IP en su. VPC Una subred debe residir en una sola zona de disponibilidad.

control de supervisión y adquisición de datos (SCADA)

En la industria manufacturera, un sistema que utiliza hardware y software para monitorear los activos físicos y las operaciones de producción.

cifrado simétrico

Un algoritmo de cifrado que utiliza la misma clave para cifrar y descifrar los datos.

pruebas sintéticas

Probar un sistema de manera que simule las interacciones de los usuarios para detectar posibles problemas o monitorear el rendimiento. Puede usar Amazon CloudWatch Synthetics para crear estas pruebas.

T

etiquetas

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos. Para obtener más información, consulte Etiquetado de los recursos de AWS.

variable de destino

El valor que intenta predecir en el ML supervisado. Esto también se conoce como variable de resultado. Por ejemplo, en un entorno de fabricación, la variable objetivo podría ser un defecto del producto.

lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

entorno de prueba

Consulte entorno.

entrenamiento

Proporcionar datos de los que pueda aprender su modelo de ML. Los datos de entrenamiento deben contener la respuesta correcta. El algoritmo de aprendizaje encuentra patrones en los datos de entrenamiento que asignan los atributos de los datos de entrada al destino (la respuesta que desea predecir). Genera un modelo de ML que captura estos patrones. Luego, el modelo de ML se puede utilizar para obtener predicciones sobre datos nuevos para los que no se conoce el destino.

puerta de enlace de tránsito

Un centro de tránsito de red que puede usar para interconectar sus VPCs redes con las locales. Para obtener más información, consulte Qué es una pasarela de tránsito en la AWS Transit Gateway documentación.

flujo de trabajo basado en enlaces troncales

Un enfoque en el que los desarrolladores crean y prueban características de forma local en una rama de característica y, a continuación, combinan esos cambios en la rama principal. Luego, la rama principal se adapta a los entornos de desarrollo, preproducción y producción, de forma secuencial.

acceso de confianza

Otorgar permisos a un servicio que especifique para realizar tareas en su organización AWS Organizations y en sus cuentas en su nombre. El servicio de confianza crea un rol vinculado al servicio en cada cuenta, cuando ese rol es necesario, para realizar las tareas de administración por usted. Para obtener más información, consulte AWS Organizations Utilización con otros AWS servicios en la AWS Organizations documentación.

ajuste

Cambiar aspectos de su proceso de formación a fin de mejorar la precisión del modelo de ML. Por ejemplo, puede entrenar el modelo de ML al generar un conjunto de etiquetas, incorporar etiquetas y, luego, repetir estos pasos varias veces con diferentes ajustes para optimizar el modelo.

equipo de dos pizzas

Un DevOps equipo pequeño al que puedes alimentar con dos pizzas. Un equipo formado por dos integrantes garantiza la mejor oportunidad posible de colaboración en el desarrollo de software.

U

incertidumbre

Un concepto que hace referencia a información imprecisa, incompleta o desconocida que puede socavar la fiabilidad de los modelos predictivos de ML. Hay dos tipos de incertidumbre: la incertidumbre epistémica se debe a datos limitados e incompletos, mientras que la incertidumbre aleatoria se debe al ruido y la aleatoriedad inherentes a los datos. Para más información, consulte la guía Cuantificación de la incertidumbre en los sistemas de aprendizaje profundo.

tareas indiferenciadas

También conocido como tareas arduas, es el trabajo que es necesario para crear y operar una aplicación, pero que no proporciona un valor directo al usuario final ni proporciona una ventaja competitiva. Algunos ejemplos de tareas indiferenciadas son la adquisición, el mantenimiento y la planificación de la capacidad.

entornos superiores

Ver entorno.

V

succión

Una operación de mantenimiento de bases de datos que implica limpiar después de las actualizaciones incrementales para recuperar espacio de almacenamiento y mejorar el rendimiento.

control de versión

Procesos y herramientas que realizan un seguimiento de los cambios, como los cambios en el código fuente de un repositorio.

VPCmirando

Una conexión entre dos VPCs que permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulta Qué es el VPC peering en la VPC documentación de Amazon.

vulnerabilidad

Defecto de software o hardware que pone en peligro la seguridad del sistema.

W

caché caliente

Un búfer caché que contiene datos actuales y relevantes a los que se accede con frecuencia. La instancia de base de datos puede leer desde la caché del búfer, lo que es más rápido que leer desde la memoria principal o el disco.

datos templados

Datos a los que el acceso es infrecuente. Al consultar este tipo de datos, normalmente se aceptan consultas moderadamente lentas.

función de ventana

SQLFunción que realiza un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para procesar tareas, como calcular una media móvil o acceder al valor de las filas en función de la posición relativa de la fila actual.

carga de trabajo

Conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend.

flujo de trabajo

Grupos funcionales de un proyecto de migración que son responsables de un conjunto específico de tareas. Cada flujo de trabajo es independiente, pero respalda a los demás flujos de trabajo del proyecto. Por ejemplo, el flujo de trabajo de la cartera es responsable de priorizar las aplicaciones, planificar las oleadas y recopilar los metadatos de migración. El flujo de trabajo de la cartera entrega estos recursos al flujo de trabajo de migración, que luego migra los servidores y las aplicaciones.

WORM

Mira, escribe una vez, lee muchas.

WQF

Consulte el marco AWS de calificación de la carga de trabajo.

escribe una vez, lee muchas (WORM)

Un modelo de almacenamiento que escribe los datos una sola vez y evita que los datos se eliminen o modifiquen. Los usuarios autorizados pueden leer los datos tantas veces como sea necesario, pero no pueden cambiarlos. Esta infraestructura de almacenamiento de datos se considera inmutable.

Z

ataque de día cero

Un ataque, normalmente de malware, que aprovecha una vulnerabilidad de día cero.

vulnerabilidad de día cero

Un defecto o una vulnerabilidad sin mitigación en un sistema de producción. Los agentes de amenazas pueden usar este tipo de vulnerabilidad para atacar el sistema. Los desarrolladores suelen darse cuenta de la vulnerabilidad a raíz del ataque.

aplicación zombi

Una aplicación que tiene un uso medio CPU de memoria inferior al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.