Mejores prácticas y funciones de cifrado para Servicios de AWS

AWS Guía prescriptiva

AWS Guía prescriptiva: Mejores prácticas y funciones de cifrado para Servicios de AWS

Table of Contents

Prácticas recomendadas y características de cifrado para los Servicios de AWS

Kurt Kumar, Amazon Web Services

Septiembre de 2024 (historia del documento)

El cifrado es una herramienta de ciberseguridad fundamental para proteger los datos confidenciales en la era digital. Dado que las organizaciones dependen cada vez más de los datos para impulsar sus operaciones, incluidas las implementaciones generativas de IA, proteger esta valiosa información mediante prácticas de cifrado sólidas es un componente esencial de una estrategia integral de protección de datos. Esta guía puede ayudarle a comprender los principios de cifrado y las capacidades de cifrado que AWS ofrece.

Las amenazas de ciberseguridad modernas incluyen el riesgo de una violación de datos, que se produce cuando el acceso no autorizado a sus activos de información provoca la pérdida de datos. Los datos son un activo empresarial exclusivo de cada organización. Puede incluir información del cliente, planes de negocios, documentos de diseño o código. Proteger la empresa significa proteger sus datos.

El cifrado de datos puede ayudar a proteger los datos de su empresa incluso después de que se produzca una infracción. Proporciona una capa de defensa contra la divulgación no intencionada. Para acceder a los datos cifrados en la Nube de AWS, los usuarios necesitan permisos a fin de utilizar la clave para descifrar y a fin de utilizar el servicio en el que se encuentran los datos. Sin estos dos permisos, los usuarios no pueden descifrar ni ver los datos.

Por lo general, hay tres tipos de datos que se pueden cifrar. Los datos en tránsito son datos que se mueven de forma activa por la red, por ejemplo, entre los recursos de la red. Los datos en reposo son datos estacionarios e inactivos, como los datos que se encuentran almacenados. Algunos ejemplos son el almacenamiento en bloques, el almacenamiento de objetos, las bases de datos, los archivos y los dispositivos de Internet de las cosas (IoT). Los datos en uso se refieren a los datos que las aplicaciones o los servicios están procesando o utilizando activamente. Al proteger los datos en el punto de uso, las organizaciones pueden ayudar a mitigar los riesgos de una divulgación no intencionada.

Esta guía analiza las consideraciones y las mejores prácticas para cifrar los datos en tránsito y los datos en reposo. También se analizan las funciones y los controles de cifrado disponibles en muchos

Servicios de AWS de ellos. Puede implementar estas recomendaciones de cifrado a nivel de servicio en sus Nube de AWS entornos.

Destinatarios previstos

A esta guía la pueden utilizar organizaciones pequeñas, medianas y grandes del sector público y privado. Tanto si su organización se encuentra en las etapas iniciales de la evaluación e implementación de una estrategia de protección de datos como si pretende mejorar los controles de seguridad existentes, las recomendaciones que se describen en esta guía son las más adecuadas para los siguientes públicos:

- Funcionarios ejecutivos que formulan políticas para su empresa, como los directores ejecutivos (CEOs), los directores de tecnología (CTOs), los directores de información (CIOs) y los directores de seguridad de la información (CISOs)
- Funcionarios de tecnología responsables de establecer los estándares técnicos, como los vicepresidentes y directores técnicos
- Las partes interesadas de la empresa y los propietarios de las aplicaciones que son responsables de:
  - Evaluar la postura de riesgo, la clasificación de los datos y los requisitos de protección
  - Monitoreo de la conformidad con los estándares organizacionales establecidos
- Funcionarios de conformidad, auditoría interna y control que se encargan de monitorear el cumplimiento de las políticas de conformidad, incluidos los regímenes de conformidad estatutarios y voluntarios

Acerca de los servicios de criptografía de AWS

Un algoritmo de cifrado es una fórmula o procedimiento que convierte un mensaje de texto sin formato en texto cifrado. Si no conoce la codificación o su terminología, le recomendamos que lea Acerca del cifrado de datos y Conceptos de criptografía antes de continuar con esta guía.

Los servicios de criptografía de AWS se basan en algoritmos de cifrado seguros y de código abierto. Organismos públicos de normalización e investigaciones académicas examinan estos algoritmos. Algunas herramientas y servicios de AWS imponen el uso de un algoritmo específico. En otros servicios, puede elegir entre varios algoritmos y longitudes de clave disponibles, o puede utilizar los valores predeterminados recomendados.

En esta sección, se describen algunos de los algoritmos que admiten las herramientas y servicios de AWS. Se dividen en dos categorías, simétricos y asimétricos, según el funcionamiento de sus claves:

- El cifrado simétrico utiliza la misma clave para cifrar y descifrar los datos. Los Servicios de AWS admiten el estándar de cifrado avanzado (AES) y el estándar de cifrado de datos triple (3DES o TDES), que son dos algoritmos simétricos muy utilizados. Para obtener más información, consulte Algoritmos simétricos en la Guía de herramientas y servicios de criptografía de AWS.
- El cifrado asimétrico 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. Los Servicios de AWS suelen admitir algoritmos asimétricos RSA y de criptografía de curva elíptica (ECC). Para obtener más información, consulte Algoritmos asimétricos en la Guía de herramientas y servicios de criptografía de AWS.

Los servicios de criptografía de AWS cumplen con una amplia gama de estándares de seguridad criptográfica, por lo que puede cumplir con las normativas gubernamentales o profesionales. Para obtener una lista completa de los estándares de seguridad de datos que cumplen los Servicios de AWS, consulte Programas de conformidad de AWS. Para obtener más información sobre las herramientas y los servicios de criptografía, consulte Herramientas y servicios de criptografía de AWS.

Prácticas recomendadas de cifrado generales

En esta sección se proporcionan recomendaciones que se aplican al cifrar datos en. Nube de AWS Estas mejores prácticas generales de cifrado no son específicas de Servicios de AWS. Esta sección se incluyen los siguientes temas:

- Clasificación de datos
- Cifrado de datos en tránsito
- Cifrado de datos en reposo

Clasificación de datos

La clasificación de datos es 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. Las categorías pueden incluir altamente confidencial, confidencial, no confidencial y público, pero los niveles de clasificación y sus nombres pueden variar de una organización a otra. Para obtener más información sobre el proceso, las consideraciones y los modelos de clasificación de datos, consulte Clasificación de datos (documentoAWS técnico).

Una vez que haya clasificado los datos, puede crear una estrategia de cifrado para su organización en función del nivel de protección requerido para cada categoría. Por ejemplo, su organización podría decidir que los datos altamente confidenciales deben utilizar un cifrado asimétrico y que los datos públicos no requieren cifrado. A fin de obtener más información sobre cómo diseñar una estrategia de cifrado, consulte Creación de una estrategia de cifrado empresarial para los datos en reposo. Si bien las consideraciones y recomendaciones técnicas de esa guía son específicas para los datos en reposo, también puede utilizar el enfoque gradual a fin de crear una estrategia de cifrado para los datos en tránsito.

Cifrado de datos en tránsito

Todos los datos que se transmiten Regiones de AWS a través de la red AWS global se cifran automáticamente en la capa física antes de que salgan de las instalaciones AWS seguras. Se cifra todo el tráfico entre las zonas de disponibilidad.

Entre estos se incluyen recomendaciones generales para cifrar datos en tránsito en la Nube de AWS:

- Defina una política de cifrado organizacional para los datos en tránsito, en función de su clasificación de datos, los requisitos organizativos y cualquier norma reglamentaria o de conformidad aplicable. Le recomendamos encarecidamente que cifre los datos en tránsito que se encuentren clasificados como altamente confidenciales o confidenciales. Su política también puede especificar el cifrado para otras categorías, como los datos públicos o no confidenciales, según sea necesario.
- Al cifrar los datos en tránsito, le recomendamos utilizar algoritmos criptográficos aprobados, modos de cifrado por bloques y longitudes de clave, como se define en su política de cifrado.
- Cifre el tráfico entre los activos y sistemas de información de la red y la Nube de AWS infraestructura corporativas mediante uno de los siguientes métodos:
  - Conexiones de AWS Site-to-Site VPN
  - Una combinación de AWS Direct Connectconexiones AWS Site-to-Site VPN y, que proporciona una conexión privada IPsec cifrada
  - AWS Direct Connect conexiones compatibles con MAC Security (MACsec) para cifrar los datos desde las redes corporativas hasta la ubicación AWS Direct Connect
- Identifique políticas de control de acceso para sus claves de cifrado en función del principio de privilegio mínimo. El privilegio mínimo es la práctica recomendada de seguridad de conceder a los usuarios el acceso mínimo que necesitan para realizar sus funciones laborales. Para obtener más información sobre la aplicación de permisos con privilegios mínimos, consulte las prácticas recomendadas de seguridad IAM y las prácticas recomendadas en materia de políticas. IAM

Cifrado de datos en reposo

Todos los servicios de almacenamiento de AWS datos, como Amazon Simple Storage Service (Amazon S3) y Amazon Elastic File System (EFSAmazon), ofrecen opciones para cifrar los datos en reposo. El cifrado se realiza mediante los servicios de cifrado y AWS criptografía por bloques del estándar de cifrado avanzado (AES-256) de 256 bits, como () o.AWS Key Management ServiceAWS KMSAWS CloudHSM

Puede cifrar los datos mediante el cifrado del lado del cliente o del lado del servidor, en función de factores como la clasificación de los datos, la necesidad de cifrado o las limitaciones técnicas que le impiden utilizar el end-to-end cifrado: end-to-end

- El cifrado del cliente es el acto de cifrar datos de forma local antes de que la aplicación o servicio de destino los reciba. El Servicio de AWS recibe los datos cifrados y no interviene en su cifrado o descifrado. En el caso del cifrado del cliente, puede utilizar AWS KMS, el AWS Encryption SDK, u otras herramientas o servicios de cifrado de terceros.
- El cifrado del servidor es el acto de cifrar datos en su destino, por la aplicación o servicio que los recibe. Para el cifrado del lado del servidor, puede utilizarlo AWS KMS para cifrar todo el bloque de almacenamiento. También puede utilizar otras herramientas o servicios de cifrado de terceros, por ejemplo, LUKSpara cifrar un sistema de archivos Linux a nivel del sistema operativo (SO).

Entre estos se incluyen prácticas recomendadas generales para cifrar datos en reposo en la Nube de AWS:

- Defina una política de cifrado organizacional para los datos en reposo, en función de su clasificación de datos, los requisitos organizativos y cualquier norma reglamentaria o de conformidad aplicable. A fin de obtener más información, consulte Creación de una estrategia de cifrado empresarial para los datos en reposo. Le recomendamos encarecidamente que cifre los datos en reposo que se encuentren clasificados como altamente confidenciales o confidenciales. Su política también puede especificar el cifrado para otras categorías, como los datos públicos o no confidenciales, según sea necesario.
- Al cifrar los datos en reposo, le recomendamos utilizar algoritmos criptográficos aprobados, modos de cifrado por bloques y longitudes de clave.
- Identifique políticas de control de acceso para sus claves de cifrado en función del principio de privilegio mínimo.

Prácticas recomendadas de cifrado para los Servicios de AWS

En esta sección se incluyen las mejores prácticas y recomendaciones para lo siguiente: Servicios de AWS

- AWS CloudTrail
- Amazon DynamoDB
- Amazon Elastic Compute Cloud (AmazonEC2) y Amazon Elastic Block Store (AmazonEBS)
- Amazon Elastic Container Registry (AmazonECR)
- Amazon Elastic Container Service (AmazonECS)
- Amazon Elastic File System (AmazonEFS)
- Servicio Amazon Elastic Kubernetes (Amazon) EKS
- AWS Encryption SDK
- AWS Key Management Service (AWS KMS)
- AWS Lambda
- Amazon Relational Database Service (AmazonRDS)
- AWS Secrets Manager
- Amazon Simple Storage Service (Amazon S3)
- Amazon Virtual Private Cloud (AmazonVPC)

Mejores prácticas de cifrado para AWS CloudTrail

AWS CloudTrail lo ayuda a auditar el control, la conformidad, el funcionamiento y el análisis de su Cuenta de AWS.

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- CloudTrail los registros deben cifrarse mediante un sistema gestionado por el cliente AWS KMS key. Elija una KMS clave que esté en la misma región que el depósito de S3 que recibe los archivos de registro. Para obtener más información, consulte Actualizar un registro para usar su KMS clave.

- Como capa de seguridad adicional, habilite la validación de los archivos de registro para los registros de seguimiento. Esto le ayuda a determinar si un archivo de registro se modificó, eliminó o no se modificó después de CloudTrail entregarlo. Para obtener instrucciones, consulte Habilitar la validación de la integridad del archivo de registro para CloudTrail.
- Utilice VPC los puntos finales de la interfaz CloudTrail para poder comunicarse con los recursos de otros VPCs sin tener que atravesar la Internet pública. Para obtener más información, consulte Uso AWS CloudTrail con puntos finales de interfaz. VPC
- Añada una clave de `aws:SourceArn` condición a la política KMS clave para asegurarse de que solo CloudTrail utilice la KMS clave para uno o varios senderos específicos. Para obtener más información, consulte Configurar AWS KMS key políticas para CloudTrail.
- En AWS Config, implemente la regla cloud-trail-encryption-enabled AWS administrada para validar y aplicar el cifrado de los archivos de registro.
- Si CloudTrail está configurado para enviar notificaciones a través de temas de Amazon Simple Notification Service (AmazonSNS), añada una clave de condición `aws:SourceArn` (u opcionalmente`aws:SourceAccount`) a la declaración de CloudTrail política para evitar el acceso no autorizado de la cuenta al SNS tema. Para obtener más información, consulte la política SNS temática de Amazon para CloudTrail.
- Si lo estás utilizando AWS Organizations, crea un registro de la organización que registre todos los eventos Cuentas de AWS de esa organización. Esto incluye la cuenta de administración y todas las cuentas de los miembros de la organización. A fin de obtener más información, consulte Creación de un registro de seguimiento para una organización.
- Cree un registro que se aplique a todos los Regiones de AWS lugares donde almacene los datos corporativos para registrar Cuenta de AWS la actividad en esas regiones. Al AWS lanzar una nueva región, incluye CloudTrail automáticamente la nueva región y registra los eventos en esa región.

Prácticas recomendadas de cifrado para Amazon DynamoDB

Amazon DynamoDB es un servicio SQL sin base de datos totalmente gestionado que proporciona un rendimiento rápido, predecible y escalable. El cifrado en reposo de DynamoDB protege los datos de una tabla cifrada, incluida su clave principal, los índices secundarios locales y globales, las transmisiones, las tablas globales, las copias de seguridad y los clústeres de DynamoDB Accelerator DAX () siempre que los datos se almacenen en un soporte duradero.

De acuerdo con los requisitos de clasificación de datos, la confidencialidad y la integridad de los datos se pueden mantener mediante la implementación del cifrado del cliente y del servidor:

En el caso del cifrado del servidor, al crear una tabla nueva, puede utilizar AWS KMS keys para cifrar la tabla. Puede usar claves AWS propias, claves administradas o claves administradas por el cliente. AWS Recomendamos utilizar claves administradas por el cliente porque su organización tiene el control total de la clave y porque cuando se utiliza este tipo de clave, la clave de cifrado a nivel de tabla, la tabla de DynamoDB, los índices secundarios locales y globales, y las transmisiones se cifran con la misma clave. Para obtener más información sobre estos tipos de claves, consulte Claves y AWS claves del cliente.

> **Note**
>
> Puede cambiar entre una clave propia, una clave AWS AWS gestionada y una clave gestionada por el cliente en cualquier momento.

Para el cifrado del lado del cliente y la end-to-end protección de los datos, tanto en reposo como en tránsito, puede utilizar el cliente de cifrado Amazon DynamoDB. Además del cifrado, que protege la confidencialidad del valor del atributo del elemento, el Cliente de encriptación de DynamoDB firma el elemento. Esto brinda protección de la integridad al permitir la detección de cambios no autorizados en el elemento, incluida la adición o eliminación de atributos o la sustitución de un valor cifrado por otro.

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- Limite los permisos a fin de deshabilitar o programar la eliminación de la clave solo para aquellos que necesiten realizar estas tareas. Estos estados impiden que todos los usuarios y el servicio DynamoDB puedan cifrar o descifrar datos y realizar operaciones de lectura y escritura en la tabla.
- Aunque DynamoDB cifra los datos en tránsito de forma predeterminada, se HTTPS recomiendan controles de seguridad adicionales. Puede utilizar cualquiera de las siguientes opciones:
  - AWS Site-to-Site VPN conexión que se utiliza para el cifradoIPsec.
  - AWS Direct Connect conexión para establecer una conexión privada.
  - AWS Direct Connect conexión con AWS Site-to-Site VPN conexión para una IPsec conexión privada cifrada.

  - Si el acceso a DynamoDB solo es necesario desde una nube privada virtual VPC (), puede usar VPC un punto de enlace de puerta de enlace y permitir que solo los recursos VPC del mismo accedan a él. Esto evita que el tráfico atraviese la Internet pública.
- Si utiliza puntos de conexión, restrinja las políticas de VPC puntos de conexión y las IAM políticas asociadas a los puntos de conexión a dichos puntos de conexión a solo los usuarios, recursos y servicios autorizados. Para obtener más información, consulte Controlar el acceso a los puntos de conexión de DynamoDB IAM mediante políticas y Controlar el acceso a los servicios mediante políticas de puntos de conexión.
- Puede implementar el cifrado de datos a nivel de columna al nivel de la aplicación para los datos que requieren cifrado, de acuerdo con su política de cifrado.
- Configure DAX los clústeres para cifrar los datos en reposo, como los datos de la caché, los datos de configuración y los archivos de registro, al momento de configurar el clúster. No puede habilitar el cifrado en reposo en un clúster existente. Este cifrado del servidor ayuda a proteger los datos del acceso no autorizado a través del almacenamiento subyacente. DAXEl cifrado en reposo se integra automáticamente AWS KMS para administrar la clave predeterminada de un solo servicio que se utiliza para cifrar los clústeres. Si no existe una clave predeterminada del servicio cuando se crea un DAX clúster cifrado, crea AWS KMS automáticamente una nueva clave AWS administrada. Para obtener más información, consulte DAXEncriptación en reposo.

  > **Note**
  >
  > Las claves administradas por el cliente no se pueden usar con DAX clústeres.

- Configure DAX los clústeres para cifrar los datos en tránsito al momento de configurar el clúster. No puede habilitar el cifrado en tránsito en un clúster existente. DAXTLSse utiliza para cifrar las solicitudes y respuestas entre la aplicación y el clúster, y utiliza el certificado x509 del clúster para autenticar la identidad del clúster. Para obtener más información, consulte DAXCifrado en tránsito.
- En AWS Config, implemente la regla dax-encryption-enabled AWS administrada para validar y mantener el cifrado de DAX los clústeres.

Mejores prácticas de cifrado para Amazon EC2 y Amazon EBS

Amazon Elastic Compute Cloud (AmazonEC2) proporciona una capacidad informática escalable en el Nube de AWS. Puede lanzar tantos servidores virtuales como necesite y escalarlos o reducirlos con rapidez. Amazon Elastic Block Store (AmazonEBS) proporciona volúmenes de almacenamiento a nivel de bloques para usarlos con EC2 instancias.

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para estos servicios:

- Etiquete todos los EBS volúmenes con la clave y el valor de clasificación de datos adecuados. Esto le ayuda a determinar e implementar los requisitos de seguridad y cifrado adecuados, de acuerdo con su política.
- De acuerdo con su política de cifrado y la viabilidad técnica, configure el cifrado de los datos en tránsito entre EC2 instancias o entre EC2 instancias y su red local.
- Cifra los EBS volúmenes de arranque y de datos de una EC2 instancia. Un EBS volumen cifrado protege los siguientes datos:
  - Datos en reposo dentro del volumen
  - Todos los datos que se mueven entre el volumen y la instancia
  - Todas las instantáneas creadas a partir del volumen
  - Todos los volúmenes creados a partir de esas instantáneas

  Para obtener más información, consulte Cómo funciona el EBS cifrado.
- Habilite el cifrado de forma predeterminada para EBS los volúmenes de su cuenta en la cuenta actual Región de AWS. Esto impone el cifrado de todos los EBS volúmenes y copias instantáneas nuevos. No afecta a los EBS volúmenes ni a las instantáneas existentes. Para obtener más información, consulte Habilitación del cifrado de manera predeterminada.
- Cifra el volumen raíz del almacén de instancias de una EC2 instancia de Amazon. Esto lo ayuda a proteger los archivos de configuración y los datos almacenados en el sistema operativo. Para obtener más información, consulta Cómo proteger los datos en reposo con el cifrado del almacén de EC2 instancias de Amazon (entrada AWS del blog)
- En AWS Config, implemente la regla de los volúmenes cifrados para automatizar las comprobaciones que validen y apliquen las configuraciones de cifrado adecuadas.

Mejores prácticas de cifrado para Amazon ECR

Amazon Elastic Container Registry (AmazonECR) es un servicio gestionado de registro de imágenes de contenedores seguro, escalable y fiable.

Amazon ECR almacena las imágenes en los depósitos de Amazon S3 que ECR gestiona Amazon. Cada ECR repositorio de Amazon tiene una configuración de cifrado, que se establece cuando se crea el repositorio. De forma predeterminada, Amazon ECR utiliza el cifrado del lado del servidor con

claves de cifrado administradas por Amazon S3 (SSE-S3). Para obtener más información, consulte Cifrado en reposo (ECRdocumentación de Amazon).

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- En lugar de utilizar el cifrado predeterminado del lado del servidor con las claves de cifrado administradas por Amazon SSE S3 (-S3), utilice las claves administradas por el cliente almacenadas en. KMS AWS KMS Este tipo de claves ofrece las opciones de control más detalladas.

  > **Note**
  >
  > La KMS clave debe estar en el mismo lugar que el repositorio. Región de AWS

- No revoques las concesiones que Amazon ECR crea de forma predeterminada al aprovisionar un repositorio. Esto puede afectar a la funcionalidad, como el acceso a los datos, el cifrado de las imágenes nuevas enviadas al repositorio o su descifrado cuando se extraen.
- Se usa AWS CloudTrail para registrar las solicitudes a las que Amazon ECR envía AWS KMS. Las entradas de registro incluyen una clave de contexto de cifrado para que sean más fáciles de identificar.
- Configura ECR las políticas de Amazon para controlar el acceso desde VPC puntos de conexión de Amazon específicos o específicosVPCs. De hecho, esto aísla el acceso de la red a un ECR recurso específico de Amazon, lo que permite el acceso solo desde ese recurso específicoVPC. Al establecer una conexión de red privada virtual (VPN) con un VPC punto de conexión de Amazon, puede cifrar los datos en tránsito.
- Amazon ECR apoya las políticas basadas en recursos. Con estas políticas, puede restringir el acceso en función de la dirección IP de origen o de la dirección IP específica. Servicio de AWS

Mejores prácticas de cifrado para Amazon ECS

Amazon Elastic Container Service (AmazonECS) es un servicio de administración de contenedores rápido y escalable que le ayuda a ejecutar, detener y administrar contenedores en un clúster.

Con AmazonECS, puedes cifrar los datos en tránsito mediante cualquiera de los siguientes enfoques:

- Cree una malla de servicios. Utilice AWS App Mesh y configure TLS las conexiones entre los proxies de Envoy desplegados y los puntos finales de malla, como nodos virtuales o puertas de

enlace virtuales. Puede utilizar TLS certificados de AWS Private Certificate Authority o certificados proporcionados por el cliente. Para obtener más información y tutoriales, consulte Habilitar el cifrado del tráfico entre servicios al AWS App Mesh usar AWS Certificate Manager (ACM) o certificados proporcionados por el cliente (entrada del blog).AWS

- Si es compatible, utilice Nitro Enclaves.AWS AWS Nitro Enclaves es una EC2 función de Amazon que permite crear entornos de ejecución aislados, denominados enclaves, a partir de instancias de Amazon. EC2 Se han diseñado para ayudar a proteger sus datos más confidenciales. Además, ACMpara Nitro Enclaves le permite utilizar TLS certificadosSSL/públicos y privados con sus aplicaciones web y servidores web que se ejecutan en EC2 instancias de Amazon con AWS Nitro Enclaves. Para obtener más información, consulte AWS Nitro Enclaves: EC2 entornos aislados para procesar datos confidenciales (entrada del blog).AWS
- Utilice el protocolo de indicación de nombres de servidor (SNI) con los balanceadores de carga de aplicaciones. Puede implementar varias aplicaciones detrás de un único agente de HTTPS escucha para un Application Load Balancer. Cada oyente tiene su propio certificado. TLS Puede proporcionar certificados o utilizar certificados autofirmados. ACM Soporta Application Load Balancer y Network Load Balancer. SNI Para obtener más información, consulte Application Load Balancers Now Support Multiple TLS Certificates with Smart Selection Using SNI (entrada AWS del blog).
- Para mejorar la seguridad y la flexibilidad, AWS Private Certificate Authority utilícelo para implementar un TLS certificado con la ECS tarea de Amazon. Para obtener más información, consulte Mantenimiento TLS completo del contenedor, parte 2: Uso AWS Private CA (entrada AWS del blog).
- Implementa mutual TLS (m TLS) en App Mesh mediante el servicio de descubrimiento secreto (Envoy) o certificados alojados en ACM (GitHub).

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- Siempre que sea técnicamente posible, para mejorar la seguridad, configure los VPCpuntos finales de la ECS interfaz de Amazon en AWS PrivateLink. Al acceder a estos puntos finales a través de una VPN conexión, se cifran los datos en tránsito.
- Almacene de forma segura los materiales confidenciales, como API claves o credenciales de bases de datos. Puede almacenarlos como parámetros cifrados en el Almacén de parámetros, una función de AWS Systems Manager. Sin embargo, te recomendamos que lo utilices, AWS Secrets Manager ya que este servicio te permite filtrar automáticamente los secretos, generar secretos aleatorios y compartirlos entre sí Cuentas de AWS.

- Para ayudar a mitigar el riesgo de fugas de datos de las variables de entorno, le recomendamos que utilice el CSIcontrolador AWS Secrets Manager y Config Provider for Secret Store (GitHub). Este controlador le permite hacer que los secretos almacenados en Secrets Manager y los parámetros almacenados en el Almacén de parámetros aparezcan como archivos montados en los pods de Kubernetes.

  > **Note**
  >
  > AWS Fargate no es compatible.

- Si los usuarios o las aplicaciones de su centro de datos o un tercero externo en la web realizan HTTPS API solicitudes directas Servicios de AWS, firme esas solicitudes con credenciales de seguridad temporales obtenidas de AWS Security Token Service (AWS STS).

Mejores prácticas de cifrado para Amazon EFS

Amazon Elastic File System (AmazonEFS) le ayuda a crear y configurar sistemas de archivos compartidos en Nube de AWS.

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- En AWS Config, implemente la regla efs-encrypted-check AWS administrada. Esta regla comprueba si Amazon EFS está configurado para cifrar los datos del archivo mediante AWS KMS.
- Aplica el cifrado de los sistemas de EFS archivos de Amazon creando una CloudWatch alarma de Amazon que monitorea CloudTrail los registros en busca de `CreateFileSystem` eventos y activa una alarma si se crea un sistema de archivos sin cifrar. Para obtener más información, consulte Tutorial: Aplicar el cifrado en un sistema de EFS archivos de Amazon en reposo.
- Monte el sistema de archivos mediante el asistente de EFSmontaje. Esto configura y mantiene un túnel TLS 1.2 entre el cliente y el EFS servicio de Amazon y enruta todo el tráfico del Network File System (NFS) a través de este túnel cifrado. El siguiente comando implementa el uso de TLS para el cifrado en tránsito.

  ```
  sudo mount -t efs  -o tls file-system-id:/ /mnt/efs
  ```

  Para obtener más información, consulte Uso EFS del asistente de montaje para montar sistemas de EFS archivos.

- Utilice AWS PrivateLink e implemente VPC puntos finales de interfaz para establecer una conexión privada entre Amazon VPCs y Amazon EFSAPI. Los datos en tránsito a través de la VPN conexión hacia y desde el punto final están cifrados. Para obtener más información, consulte Acceso y Servicio de AWS uso de un VPC punto final de interfaz.
- Utilice la clave de `elasticfilesystem:Encrypted` condición en las políticas IAM basadas en la identidad para evitar que los usuarios creen sistemas de EFS archivos que no estén cifrados. Para obtener más información, consulte Utilización IAM para forzar la creación de sistemas de archivos cifrados.
- KMSlas claves utilizadas para el EFS cifrado deben configurarse para un acceso con privilegios mínimos mediante políticas de claves basadas en los recursos.
- Utilice la clave de `aws:SecureTransport` condición de la política del sistema de EFS archivos para obligar a los NFS clientes a utilizarla cuando se conecten a un sistema de TLS archivos. EFS Para obtener más información, consulte Cifrado de datos en tránsito en Cifrado de datos de archivos con Amazon Elastic File System (AWS documento técnico).

Mejores prácticas de cifrado para Amazon EKS

Amazon Elastic Kubernetes Service (EKSAmazon) le ayuda a ejecutar AWS Kubernetes sin necesidad de instalar o mantener su propio plano de control o nodos de Kubernetes. En Kubernetes, los secretos le ayudan a administrar la información confidencial, como los certificados de usuario, las contraseñas o las claves. API De forma predeterminada, estos secretos se almacenan sin cifrar en el almacén de datos subyacente del API servidor, que se denomina etcd. Cualquier usuario con API acceso o acceso a `etcd` puede recuperar o modificar un secreto. Además, cualquier persona autorizada a crear un pod en un espacio de nombres puede utilizar ese acceso para leer cualquier secreto de ese espacio de nombres. Puedes cifrar estos secretos inactivos en Amazon EKS mediante claves AWS KMS keys gestionadas o claves AWS gestionadas por el cliente. Un enfoque alternativo `etcd` es usar AWS Secrets and Config Provider (ASCP) (GitHub repositorio). ASCPse integra con IAM políticas basadas en recursos para limitar y restringir el acceso a los secretos solo dentro de determinados pods de Kubernetes dentro de un clúster.

Puedes usar los siguientes AWS servicios de almacenamiento con Kubernetes:

- Para Amazon Elastic Block Store (AmazonEBS), puede utilizar el controlador de almacenamiento en árbol o el controlador de Amazon EBS CSI. Ambos incluyen parámetros para cifrar los volúmenes y brindar una clave administrada por el cliente.

- En el caso de Amazon Elastic File System (AmazonEFS), puede utilizar el EFSCSIcontrolador Amazon compatible con el aprovisionamiento dinámico y estático.

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- Si utiliza `etcd`, que almacena los objetos secretos sin cifrar de forma predeterminada, realice lo siguiente para ayudar a proteger los secretos:
  - Cifrar los datos secretos en reposo (documentación de Kubernetes).
  - Habilite o configure la autorización mediante reglas de control de acceso basadas en roles (RBAC) que restringen la lectura y la escritura del secreto. Restrinja los permisos para crear secretos nuevos o reemplazar los existentes. Para obtener más información, consulte Información general sobre la autorización (documentación de Kubernetes).
  - Si define varios contenedores en un pod y solo uno de ellos necesita acceder a un secreto, defina el montaje del volumen para que los demás contenedores no tengan acceso a ese secreto. Los secretos que se montan como volúmenes se instancian como volúmenes `tmpfs` y se eliminan de forma automática del nodo cuando se elimina el pod. También puede utilizar variables de entorno, pero no recomendamos este enfoque porque los valores de las variables de entorno pueden aparecer en los registros. Para obtener más información, consulte Secretos (documentación de Kubernetes).
  - Cuando sea posible, evite conceder acceso a las solicitudes `watch` y `list` para secretos dentro de un espacio de nombres. En KubernetesAPI, estas solicitudes son eficaces porque permiten al cliente inspeccionar los valores de cada secreto de ese espacio de nombres.
  - Permita que solo los administradores de clústeres accedan a `etcd`, incluido el acceso de solo lectura.
  - Si hay varias `etcd` instancias, asegúrate de TLS utilizarlas para la comunicación `etcd` entre pares. `etcd`
- Si lo está utilizandoASCP, haga lo siguiente para ayudar a proteger los secretos:
  - Usa IAMfunciones en las cuentas de servicio para limitar el acceso secreto solo a los pods autorizados.
  - Habilite el cifrado de los secretos de Kubernetes mediante el proveedor de AWS cifrado (GitHub repositorio) para implementar el cifrado de sobres con una clave gestionada por el cliente. KMS
- Crea un filtro de CloudWatch métricas y una alarma de Amazon para enviar alertas sobre operaciones especificadas por el administrador, como la eliminación de un secreto o el uso de una

versión secreta en el período de espera para eliminarlo. Para obtener más información, consulte Creación de una alarma basada en la detección de anomalías.

Mejores prácticas de cifrado para AWS Encryption SDK

El AWS Encryption SDK es una biblioteca de cifrado del cliente de código abierto. Utiliza los estándares del sector y las mejores prácticas para respaldar la implementación y la interoperabilidad en varios lenguajes de programación. AWS Encryption SDK cifra los datos mediante un algoritmo de clave simétrica, autenticado y seguro, y ofrece una implementación predeterminada que se ajusta a las mejores prácticas de criptografía. Para obtener más información, consulte los Conjuntos de algoritmos admitidos en el AWS Encryption SDK.

Una de las principales características del AWS Encryption SDK es la compatibilidad con el cifrado de los datos en uso. Al adoptar un encrypt-then-use enfoque, puede cifrar los datos confidenciales antes de que la lógica de la aplicación los procese. Esto puede ayudar a proteger los datos de una posible exposición o manipulación, incluso si la propia aplicación se ve afectada por un problema de seguridad.

Tenga en cuenta las siguientes prácticas recomendadas para este servicio:

- Cumpla con todas las recomendaciones de las Prácticas recomendadas para el AWS Encryption SDK.
- Seleccione una o más claves de encapsulamiento para ayudar a proteger sus claves de datos. Para obtener más información, consulte Seleccionar las claves de encapsulamiento.
- Transfiera el `KeyId` parámetro a la ReEncryptoperación para evitar el uso de una clave que no sea de confianzaKMS. Para obtener más información, consulte Cifrado mejorado del lado del cliente: compromiso explícito KeyIds y clave (AWS entrada del blog).
- Cuando utilice el AWS Encryption SDK con AWS KMS, utilice el filtrado local`KeyId`. Para obtener más información, consulte Cifrado mejorado del lado del cliente: compromiso explícito KeyIds y clave (entrada del AWS blog).
- Para las aplicaciones con grandes volúmenes de tráfico que requieren cifrado o descifrado, o si su cuenta supera las cuotas de AWS KMS solicitudes, puede utilizar la función de almacenamiento en caché de claves de datos del. AWS Encryption SDK Tenga en cuenta las siguientes prácticas recomendadas para el almacenamiento en caché de las claves de datos:
  - Configure los umbrales de seguridad de la caché para limitar el tiempo durante el cual se utiliza cada clave de datos almacenada en caché, así como la cantidad de datos que se protegen

con cada una de ellas. Para obtener recomendaciones a la hora de configurar estos umbrales, consulte Configuración de los umbrales de seguridad de la caché.

- Limite la caché local a la cantidad mínima de claves de datos necesaria a fin de lograr las mejoras de rendimiento para el caso de uso específico de su aplicación. Para obtener instrucciones y un ejemplo de cómo configurar los límites de la caché local, consulte Uso del almacenamiento en caché de claves de datos:. Step-by-step

Para obtener más información, consulte AWS Encryption SDK: Cómo decidir si el almacenamiento en caché de claves de datos es adecuado para su aplicación (entrada del AWS blog).

Mejores prácticas de cifrado para AWS Key Management Service

AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos. AWS KMS se integra con la mayoría de los Servicios de AWS dispositivos que pueden cifrar sus datos. Para obtener una lista completa, consulte Servicios de AWS integrado con AWS KMS. AWS KMS también se integra con AWS CloudTrail el fin de registrar el uso de sus KMS claves para necesidades de auditoría, normativas y de cumplimiento.

KMSlas claves son el recurso principal y son representaciones lógicas de una clave criptográfica. AWS KMS Existen tres tipos principales de KMS claves:

- Las claves administradas por el cliente son KMS claves que usted crea.
- AWS las claves gestionadas son KMS claves que se Servicios de AWS crean en tu cuenta y en tu nombre.
- AWS las claves propias son KMS claves que una persona Servicio de AWS posee y administra, para usarlas en múltiples ocasiones Cuentas de AWS.

Para obtener más información sobre estos tipos de claves, consulte Claves del cliente y claves de AWS.

En el Nube de AWS, las políticas se utilizan para controlar quién puede acceder a los recursos y servicios. Por ejemplo, en AWS Identity and Access Management (IAM), las políticas basadas en la identidad definen los permisos para los usuarios, los grupos de usuarios o las funciones, y las políticas basadas en recursos se asocian a un recurso, como un bucket de S3, y definen a qué entidades principales se les permite el acceso, las acciones admitidas y cualquier otra condición que deba cumplirse. Al igual que las IAM políticas, AWS KMS utiliza políticas clave para controlar el acceso a una clave. KMS Cada KMS clave debe tener una política clave y cada clave solo puede

tener una política clave. Tenga en cuenta lo siguiente al definir las políticas que permiten o deniegan el acceso a KMS las claves:

- Puede controlar la política clave para las claves administradas por el cliente, pero no puede controlar directamente la política clave para las claves AWS administradas o las claves AWS propias.
- Las políticas clave permiten conceder un acceso detallado a las AWS KMS API llamadas dentro de un Cuenta de AWS. A menos que la política clave lo permita explícitamente, no puede usar IAM políticas para permitir el acceso a una KMS clave. Sin el permiso de la política clave, IAM las políticas que permiten permisos no tienen ningún efecto. Para obtener más información, consulte Permitir IAM políticas que permitan el acceso a la KMS clave.
- Puede utilizar una IAM política para denegar el acceso a una clave gestionada por el cliente sin el correspondiente permiso de la política de claves.
- Al diseñar políticas clave y IAM políticas para claves multirregionales, tenga en cuenta lo siguiente:
  - Las políticas de claves no son propiedades compartidas de claves de varias regiones y no se copian ni sincronizan entre las claves de varias regiones relacionadas.
  - Cuando se crea una clave de varias regiones mediante las acciones `CreateKey` y `ReplicateKey`, se aplica la política de claves predeterminada a menos que se especifique una política de claves en la solicitud.
  - Puede implementar claves de condición, como aws: RequestedRegion, para limitar los permisos a una determinada Región de AWS.
  - Puede utilizar concesiones para dar permisos a una clave principal de varias regiones o clave de réplica. Sin embargo, no se puede utilizar una sola concesión para conceder permisos a varias KMS claves, aunque estén relacionadas con claves multirregionales.

Al utilizar AWS KMS y crear políticas de claves, tenga en cuenta las siguientes prácticas recomendadas de cifrado y otras prácticas recomendadas de seguridad:

- Siga las recomendaciones de los siguientes recursos para conocer las AWS KMS mejores prácticas:
  - Mejores prácticas en materia de AWS KMS subvenciones (AWS KMS documentación)
  - Mejores prácticas en materia de IAM políticas (AWS KMS documentación)
- De acuerdo con la práctica recomendada de separación de funciones, mantenga identidades separadas para quienes administran las claves y quienes las utilizan:
  - Los roles de administrador que crean y eliminan claves no deberían poder utilizarlas.

  - Es posible que algunos servicios solo necesiten cifrar los datos y no se les debe permitir descifrar los datos con la clave.
- Las políticas de claves siempre deben seguir un modelo de privilegio mínimo. No la use `kms:*` para acciones IAM o políticas clave, ya que esto otorga al principal permisos tanto para administrar como para usar la clave.
- Limite el uso de claves administradas por el cliente a un Servicios de AWS número específico mediante la clave de ViaService condición kms: incluida en la política de claves.
- Si puede elegir entre los tipos de claves, se prefieren las claves administradas por el cliente porque brindan las opciones de control más detalladas, incluidas las siguientes:
  - Administración de la autenticación y el control de acceso
  - Habilitación y deshabilitación de claves
  - Rotación de AWS KMS keys
  - Etiquetado de claves
  - Creación de alias
  - Eliminación de AWS KMS keys
- AWS KMS Los permisos administrativos y de modificación deben denegarse explícitamente a los titulares no aprobados y los permisos de AWS KMS modificación no deben figurar en una declaración de autorización para los titulares no autorizados. Para obtener información, consulte Acciones, recursos y claves de condición de AWS Key Management Service.
- Para detectar el uso no autorizado de KMS claves, implemente las reglas AWS Config-kms-actions y iam-customer-policy-blocked-kms-actions. iam-inline-policy-blocked Esto impide que los directores utilicen las acciones de descifrado en todos los recursos. AWS KMS
- Implemente políticas de control de servicios (SCPs) AWS Organizations para evitar que usuarios o roles no autorizados eliminen KMS las claves, ya sea directamente como un comando o a través de la consola. Para obtener más información, consulte Uso SCPs como controles preventivos (AWS entrada del blog).
- Registra AWS KMS API las llamadas en un CloudTrail registro. Esto registra los atributos del evento relevantes, como las solicitudes que se realizaron, la dirección IP de origen desde la que se realizó la solicitud y quién la realizó. Para obtener más información, consulte Registrar AWS KMS API llamadas con AWS CloudTrail.
- Si utilizas un contexto de cifrado, no debería contener información confidencial. CloudTrail almacena el contexto de cifrado en JSON archivos de texto sin formato, que pueden ser

consultados por cualquier persona que tenga acceso al depósito de S3 que contiene la información.

- Cuando monitoree el uso de las claves administradas por el cliente, configure los eventos para que lo notifiquen si se detectan acciones específicas, como la creación de claves, las actualizaciones de las políticas de claves administradas por el cliente o la importación de material clave. También se recomienda implementar respuestas automatizadas, como una función de AWS Lambda que deshabilita la clave o realiza cualquier otra acción de respuesta a incidentes según lo dicten las políticas de la organización.
- Se recomiendan las claves de varias regiones para situaciones específicas, como la conformidad, la recuperación de desastres o las copias de seguridad. Las propiedades de seguridad de las claves de varias regiones son significativamente diferentes de las claves de una sola región. Las siguientes recomendaciones se aplican a la hora de autorizar la creación, la administración y el uso de claves de varias regiones:
  - Permita a las entidades principales replicar una clave de varias regiones solo en las Regiones de AWS que las requieran.
  - De permiso para las claves de varias regiones solo a las entidades principales que las necesiten y solo para las tareas que las requieran.

Mejores prácticas de cifrado para AWS Lambda

AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. A fin de proteger las variables de entorno, puede utilizar el cifrado en el servidor para proteger los datos en reposo y el cifrado del lado del cliente para proteger los datos en tránsito.

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- Lambda siempre proporciona cifrado en el servidor en reposo con una AWS KMS key. De forma predeterminada, Lambda usa una clave AWS administrada. Le recomendamos que utilice una clave administrada por el cliente porque tiene el control total sobre la clave, incluida la administración, la rotación y la auditoría.
- Para los datos en tránsito que requieren cifrado, habilite los ayudantes, lo que garantiza que las variables de entorno estén cifradas en el lado del cliente para protegerlas en tránsito mediante la clave preferida. KMS Para obtener más información, consulte Seguridad en tránsito en Protección de variables de entorno.

- Las variables de entorno de la función de Lambda que contienen datos confidenciales o críticos deben cifrarse en tránsito para ayudar a proteger los datos que se transmiten de forma dinámica a las funciones (por lo general, información de acceso) del acceso no autorizado.
- Para evitar que un usuario vea las variables de entorno, añada una declaración a los permisos del usuario en la IAM política o en la política clave que deniegue el acceso a la clave predeterminada, a una clave administrada por el cliente o a todas las claves. Para obtener más información, consulte Uso de variables de entorno de AWS Lambda.

Mejores prácticas de cifrado para Amazon RDS

Amazon Relational Database Service (RDSAmazon) le ayuda a configurar, operar y escalar una base de datos relacional (DB) en el. Nube de AWS Los datos cifrados en reposo incluyen el almacenamiento subyacente de las instancias de base de datos, sus copias de seguridad automatizadas, sus réplicas de lectura y sus instantáneas.

Los siguientes son los enfoques que puede utilizar para cifrar los datos en reposo en RDS las instancias de base de datos:

- Puede cifrar las instancias de Amazon RDS DB con AWS KMS keys una clave gestionada o una clave AWS gestionada por el cliente. Para obtener más información, consulte la sección AWS Key Management Service de esta guía.
- Amazon RDS for Oracle y Amazon RDS for SQL Server admiten el cifrado de instancias de base de datos con Transparent Data Encryption (TDE). Para obtener más información, consulte Oracle Transparent Data Encryption o Support for Transparent Data Encryption in SQL Server.

  Puede utilizar ambas KMS claves para cifrar TDE las instancias de base de datos. Sin embargo, esto puede afectar levemente al rendimiento de la base de datos y debe administrar estas claves por separado.

Los siguientes son los enfoques que puede utilizar para cifrar los datos en tránsito hacia o desde las instancias de RDS base de datos:

- En el caso de una instancia de Amazon RDS DB que ejecute MariaDB, SQL Microsoft ServerSQL, My, Oracle SQL o Postgre, SSL puede utilizarla para cifrar la conexión. Para obtener más información, consulte Uso deSSL/para cifrar una conexión TLS a una instancia de base de datos.
- Amazon RDS for Oracle también admite el cifrado de red nativo de Oracle (NNE), que cifra los datos a medida que se mueven hacia y desde una instancia de base de datos. NNEy el SSL

cifrado no se puede utilizar simultáneamente. Para obtener más información, consulte Oracle Native Network Encryption.

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- Cuando se conecte a SQL instancias de base de datos de Amazon RDS RDS for SQL Server o Amazon for Postgre para procesar, almacenar o transmitir datos que requieren cifrado, utilice la función RDS Transport Encryption para cifrar la conexión. Puede implementarlo al establecer el parámetro `rds.force_ssl` en `1` en el grupo de parámetros. Para obtener más información, consulte Trabajo con los grupos de parámetros. Amazon RDS for Oracle utiliza el cifrado de red nativo de la base de datos de Oracle.
- Las claves administradas por el cliente para el cifrado de RDS instancias de base de datos deben usarse únicamente con ese propósito y no con ningún otro Servicios de AWS.
- Antes de cifrar una RDS instancia de base de datos, establezca los requisitos KMS clave. La clave que se utiliza en la instancia no se puede cambiar más adelante. Por ejemplo, en su política de cifrado, defina los estándares de uso y administración para las claves AWS administradas o las claves administradas por el cliente, en función de los requisitos de su empresa.
- Al autorizar el acceso a una KMS clave gestionada por el cliente, siga el principio del mínimo privilegio mediante el uso de claves de condición en las políticas. IAM Por ejemplo, para permitir que una clave gestionada por el cliente se utilice únicamente para solicitudes que se originen en AmazonRDS, utiliza la clave de ViaService condición kms: con el `rds.<region>.amazonaws.com` valor. Además, puedes usar claves o valores en el contexto de RDS cifrado de Amazon como condición para usar la clave gestionada por el cliente.
- Se recomienda encarecidamente activar las copias de seguridad de las RDS instancias de bases de datos cifradas. Amazon RDS puede perder el acceso a la KMS clave de una instancia de base de datos, por ejemplo, cuando la KMS clave no está habilitada o cuando se revoca el RDS acceso a una KMS clave. Si esto ocurre, la instancia de base de datos cifrada pasa a un estado de recuperación durante siete días. Si la instancia de base de datos no recupera el acceso a la clave después de siete días, la base de datos pasa a ser inaccesible desde el punto de vista de terminal y se debe restaurar a partir de una copia de seguridad. Para obtener más información, consulte Cifrado de una instancia de base de datos.
- Si una réplica de lectura y su instancia de base de datos cifrada se encuentran en la misma ubicación Región de AWS, debe utilizar la misma KMS clave para cifrar ambas.

- En AWS Config, implemente la regla rds-storage-encrypted AWS administrada para validar y aplicar el cifrado de las RDS instancias de base de datos y la rds-snapshots-encryptedregla para validar y aplicar el cifrado de las instantáneas de RDS bases de datos.
- Úselo AWS Security Hub para evaluar si sus RDS recursos de Amazon siguen las mejores prácticas de seguridad. Para obtener más información, consulta los controles de Security Hub para Amazon RDS.

Mejores prácticas de cifrado para AWS Secrets Manager

AWS Secrets Managerle ayuda a reemplazar las credenciales codificadas en su código, incluidas las contraseñas, con una API llamada a Secrets Manager para recuperar el secreto mediante programación. Secrets Manager se integra AWS KMS para cifrar cada versión de cada valor secreto con una clave de datos única que está protegida por un AWS KMS key. Esta integración protege los secretos almacenados con claves de cifrado que nunca quedan AWS KMS sin cifrar. También puede definir permisos personalizados en la KMS clave para auditar las operaciones que generan, cifran y descifran las claves de datos que protegen los secretos almacenados. Para obtener más información, consulte Cifrado y descifrado de secretos en AWS Secrets Manager.

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- En la mayoría de los casos, se recomienda utilizar la clave `aws/secretsmanager` AWS gestionada para cifrar los secretos. Su uso no conlleva ningún coste.
- Para poder acceder a un secreto desde otra cuenta o aplicar una política de claves a la clave de cifrado, utilice una clave gestionada por el cliente para cifrar el secreto.
  - En la política de claves, asigne el valor `secretsmanager.<region>.amazonaws.com` a la clave de ViaService condición kms:. Esto limita el uso de la clave solo a las solicitudes de Secrets Manager.
  - Para limitar aún más el uso de la clave a las solicitudes de Secrets Manager con el contexto correcto, utilice claves o valores del contexto de cifrado de Secrets Manager como condición para usar la KMS clave creando:
    - Un operador de condición de cadena en una IAM política o política clave
    - Una restricción de la concesión en una concesión

Prácticas recomendadas de cifrado para Amazon S3

Amazon Simple Storage Service (Amazon S3) es un servicio de almacenamiento de objetos basado en la nube que lo ayuda a almacenar, proteger y recuperar cualquier cantidad de datos.

Para el cifrado del servidor en Amazon S3, hay tres opciones:

- Cifrado del lado del servidor con claves de cifrado administradas por Amazon S3 (-S3) SSE
- Cifrado del lado del servidor con (-) AWS Key Management Service SSE KMS
- Cifrado del lado del servidor con claves de cifrado proporcionadas por el cliente (-C) SSE

Amazon S3 aplica el cifrado del lado del servidor con claves administradas de Amazon SSE S3 (-S3) como nivel base de cifrado para cada bucket de Amazon S3. Desde el 5 de enero de 2023, todas las cargas de objetos nuevos a Amazon S3 se cifran automáticamente sin costo adicional y sin afectar al rendimiento. El estado de cifrado automático para la configuración de cifrado predeterminada del bucket S3 y para la carga de nuevos objetos está disponible en AWS CloudTrail los registros, S3 Inventory, S3 Storage Lens, la consola de Amazon S3 y como encabezado de API respuesta adicional de Amazon S3 en AWS Command Line Interface (AWS CLI) y AWS SDKs. Para obtener más información, consulte Cifrado FAQ predeterminado.

Si se utiliza el cifrado del lado del servidor para cifrar un objeto en el momento de la carga, añada el `x-amz-server-side-encryption` encabezado a la solicitud para indicar a Amazon S3 que cifre el objeto mediante SSE -S3, SSE - o -C. KMS SSE Los valores posibles del encabezado son los siguientes: `x-amz-server-side-encryption`

- `AES256`, que le indica a Amazon S3 que utilice las claves administradas por Amazon S3.
- `aws:kms`, que indica a Amazon S3 que utilice claves AWS KMS administradas.
- Establecer el valor como `True` o `False` para SSE -C

Para obtener más información, consulte el Defense-in-depth requisito 1: Los datos deben estar cifrados en reposo y durante el tránsito en How to Use Bucket Policies and Apply Defense-in-Depth to Help Secure Your Amazon S3 Data (entrada del AWS blog).

Para el cifrado del cliente en Amazon S3, hay dos opciones:

- Una clave almacenada en AWS KMS
- Una clave que se almacena en la aplicación

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- En AWS Config, implemente la regla AWS administrada bucket-server-side-encryptionhabilitada para S3 para validar y aplicar el cifrado de buckets de S3.
- Implemente una política de bucket de Amazon S3 que valide que todos los objetos que se cargan se encuentren cifrados mediante la condición `s3:x-amz-server-side-encryption`. Para obtener más información, consulta el ejemplo de política de bucket en Proteger los datos mediante SSE -S3 y las instrucciones en Añadir una política de bucket.
- Permita solo las conexiones cifradas a través de HTTPS (TLS) mediante la `aws:SecureTransport` condición de las políticas de bucket de S3. Para obtener más información, consulta ¿Qué política de buckets de S3 debo usar para cumplir con la AWS Config regla s3-bucket-ssl-requests-only?
- En AWS Config, implemente la regla bucket-ssl-requests-only AWS administrada por s3 para exigir su uso a las solicitudesSSL.
- Utilice una clave administrada por el cliente si debe conceder acceso entre cuentas a sus objetos de Amazon S3. Configure la política de claves para que permita el acceso desde otra Cuenta de AWS.

Mejores prácticas de cifrado para Amazon VPC

Amazon Virtual Private Cloud (AmazonVPC) le ayuda a lanzar AWS recursos en una red virtual que haya definido. Esa red virtual es similar a la red tradicional que utiliza en su propio centro de datos, con los beneficios de utilizar la infraestructura escalable de AWS.

Tenga en cuenta las siguientes prácticas recomendadas de cifrado para este servicio:

- Cifre el tráfico entre los activos y sistemas de información dentro de la red corporativa VPCs mediante uno de los siguientes métodos:
  - AWS Site-to-Site VPN conexiones
  - Una combinación de AWS Direct Connect conexiones AWS Site-to-Site VPN y, que proporciona una IPsec conexión privada cifrada
  - AWS Direct Connect conexiones compatibles con MAC Security (MACsec) para cifrar los datos desde las redes corporativas hasta la ubicación AWS Direct Connect
- Utilice VPC los puntos finales para conectarse de forma privada AWS PrivateLink a los compatibles Servicios de AWS sin utilizar una puerta de enlace VPCs a Internet. Puede utilizar nuestros AWS Direct Connect AWS VPN servicios para establecer esta conexión. El tráfico entre

su servicio VPC y el otro no sale de la AWS red. Para obtener más información, consulte Acceder a Servicios de AWS través de AWS PrivateLink.

- Configure las reglas de los grupos de seguridad que permitan el tráfico únicamente desde los puertos asociados a protocolos seguros, por ejemplo, HTTPS por encima de TCP /443. Audite de forma periódica los grupos de seguridad y sus reglas.

Recursos

- Creación de una estrategia empresarial de cifrado para los datos en reposo (orientación AWS prescriptiva)
- Mejores prácticas de seguridad para AWS Key Management Service (AWS KMS documentación)
- Cómo Servicios de AWS usarlo AWS KMS (AWS KMS documentación)
- Pilar de seguridad: protección de datos (AWS Well-Architected Framework)

Historial de documentos

En la siguiente tabla, se describen cambios significativos de esta guía. Si quieres recibir notificaciones sobre futuras actualizaciones, puedes suscribirte a un RSSfeed.

Cambio	Descripción	Fecha
Actualizaciones de Secrets Manager	Actualizamos la información y las recomendaciones para AWS Secrets Manager.	9 de septiembre de 2024
Servicio de AWS actualizaciones	Hemos actualizado la información y las recomendaciones para Amazon Elastic Kubernetes Service (EKSAmazon), Amazon Relational Database Service (Amazon AWS Encryption SDK) y RDS Amazon Simple Storage Service (Amazon S3).	4 de septiembre de 2024
Publicación inicial	—	2 de diciembre 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 un 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

Una 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 se tiene confianza, se despliega la nueva versión y se 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 Bitbucket Cloud. 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 gestión de la 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. CI/CD is commonly described as a pipeline. CI/CDpueden 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

Vea la 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 administración y 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, las cuestiones AWS CAF de 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 el 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 la sección 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, parchear 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 de AWS cuentas múltiples, una 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 e Internet en general.

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 la 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`, por lo general, 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.

publish/subscribe (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.