AWS Key Management Service mejores prácticas

AWS Guía prescriptiva

AWS Guía prescriptiva: AWS Key Management Service mejores prácticas

Table of Contents

AWS Key Management Service mejores prácticas

Amazon Web Services (colaboradores)

Marzo de 2025 (historial del documento)

AWS Key Management Service (AWS KMS) es un servicio administrado que le facilita la creación y el control de las claves criptográficas que se utilizan para proteger los datos. Esta guía describe cómo usarlo de manera efectiva AWS KMS y proporciona las mejores prácticas. Le ayuda a comparar las opciones de configuración y a elegir el conjunto que mejor se adapte a sus necesidades.

Esta guía incluye recomendaciones sobre cómo su organización puede utilizar AWS KMS para proteger la información confidencial e implementar la firma en varios casos de uso. Considera las recomendaciones actuales que utilizan las siguientes dimensiones:

- Administración de claves: opciones de delegación para las opciones de administración y almacenamiento de claves
- Protección de datos: cifrar los datos dentro de sus propias aplicaciones en lugar de Servicios de AWS hacerlo en su nombre
- Gestión del acceso: utilizar políticas AWS KMS clave y políticas AWS Identity and Access Management (IAM) para implementar el control de acceso basado en roles (RBAC) o el control de acceso basado en atributos (ABAC).
- Arquitectura multicuenta y multiregión: recomendaciones para despliegues a gran escala.
- Administración de costos y facturación: conozca sus costos y su uso, y recomiende formas de reducir los costos.
- Controles de Detective: supervisan el estado de las claves KMS, la configuración de cifrado y los datos cifrados.
- Respuesta a incidentes: corregir los errores de configuración que provocan el incumplimiento de las políticas de protección de datos.

Resultados empresariales específicos

Sus datos son un activo fundamental y confidencial para su empresa. Con AWS KMSél, usted administra las claves criptográficas que se utilizan para proteger y verificar sus datos. Usted controla cómo se utilizan sus datos, quién tiene acceso a ellos y cómo se cifran. El objetivo de esta guía

es ayudar a los desarrolladores, administradores de sistemas y profesionales de la seguridad a implementar las mejores prácticas de cifrado que ayuden a proteger los datos confidenciales que se almacenan o se transmiten a través de ellos Servicios de AWS. Si comprende e implementa las recomendaciones de esta guía, podrá promover la confidencialidad e integridad de los datos en todo su AWS entorno. Puede cumplir con sus requisitos de protección de datos, tanto si dichos requisitos se formulan internamente como si tiene requisitos específicos para un programa de conformidad o validación. Para obtener más información sobre cómo AWS KMS puede ayudarle a proteger los datos de su AWS entorno, consulte Uso del AWS KMS cifrado Servicios de AWS en la AWS KMS documentación.

Acerca AWS KMS keys

AWS Key Management Service (AWS KMS) le permite crear claves criptográficas que se pueden utilizar en los datos que se transfieran al servicio. El tipo de recurso principal es la clave KMS, de la que hay tres tipos:

- Claves simétricas del estándar de cifrado avanzado (AES): son claves de 256 bits que se utilizan en el modo Galois Counter Mode (GCM) del AES. Estas claves proporcionan cifrado y descifrado autenticados de datos con un tamaño inferior a 4 KB. Este es el tipo de clave más común. Se utiliza para proteger otras claves de datos, como las que se utilizan en sus aplicaciones, o las Servicios de AWS que cifran los datos en su nombre.
- Claves asimétricas RSA o de curva elíptica: estas claves están disponibles en varios tamaños y admiten muchos algoritmos. Según el algoritmo, se pueden usar para cifrar y descifrar y para operaciones de firma y verificación.
- Claves simétricas para realizar operaciones con códigos de autenticación de mensajes (HMAC) basadas en hash: estas claves son claves de 256 bits que se utilizan para las operaciones de firma y verificación.

Las claves KMS no se pueden exportar desde el servicio en texto sin formato. Las generan los módulos de seguridad de hardware (HSMs) utilizados por el servicio y solo se pueden usar dentro de ellos. Esta es una propiedad de seguridad fundamental AWS KMS para evitar que las claves se vean comprometidas. En las regiones de China (Beijing) y China (Ningxia), HSMs están certificadas por la OSCCA. En todas las demás regiones, las HSMs utilizadas se AWS KMS validan según el programa FIPS 140 del NIST con un nivel de seguridad 3. Para obtener más información sobre el diseño y los controles AWS KMS que ayudan a proteger sus claves, consulte Detalles AWS Key Management Service criptográficos.

Puede enviar datos AWS KMS mediante varios tipos de criptografía APIs para realizar operaciones de cifrado, descifrado, firma o verificación con claves KMS. También puede elegir que una clave KMS actúe como clave de cifrado, lo que protege un tipo de clave denominado clave de datos. Puede exportar una clave de datos AWS KMS para utilizarla en su aplicación local o desde una Servicio de AWS que proteja los datos en su nombre. El uso de claves de datos es común en todos los sistemas de administración de claves y, a menudo, se denomina cifrado sobre. El cifrado de sobres permite utilizar una clave de datos en el sistema remoto que gestiona los datos confidenciales, en lugar de tener que enviarlos al sistema remoto AWS KMS para su cifrado directamente con una clave KMS.

Para obtener más información, consulte AWS KMS keyslos aspectos básicos de AWS KMS la criptografía en la AWS KMS documentación.

Mejores prácticas de administración clave para AWS KMS

Cuando AWS Key Management Service utilices (AWS KMS), debes tomar algunas decisiones fundamentales de diseño. Estas incluyen si se debe utilizar un modelo centralizado o descentralizado para la administración y el acceso a las claves, el tipo de claves que se deben utilizar y el tipo de almacén de claves que se van a utilizar. Las siguientes secciones le ayudan a tomar las decisiones adecuadas para su organización y sus casos de uso. Esta sección concluye con consideraciones importantes para deshabilitar y eliminar las claves de KMS, incluidas las medidas que debe tomar para ayudar a proteger sus datos y claves.

Esta sección contiene los siguientes temas:

- Elegir un modelo centralizado o descentralizado
- Elegir claves administradas por el cliente, claves AWS administradas o claves AWS propias
- Elegir un almacén de AWS KMS claves
- Eliminar y deshabilitar las claves de KMS

Elegir un modelo centralizado o descentralizado

AWS recomienda utilizar varias cuentas Cuentas de AWS y administrarlas como una sola organización en AWS Organizations. Existen dos enfoques generales para la administración AWS KMS keys en entornos de múltiples cuentas.

El primer enfoque es un enfoque descentralizado, en el que se crean claves en cada cuenta que utilice esas claves. Al almacenar las claves de KMS en las mismas cuentas que los recursos que protegen, resulta más fácil delegar los permisos a los administradores locales, que conocen los requisitos de acceso de sus AWS entidades principales y claves. Puede autorizar el uso de claves utilizando solo una política clave, o puede combinar una política clave y políticas basadas en la identidad AWS Identity and Access Management (IAM).

El segundo enfoque es un enfoque centralizado, en el que se mantienen las claves de KMS en una o varias designadas. Cuentas de AWS Permites que otras cuentas solo usen las claves para operaciones criptográficas. Usted administra las claves, su ciclo de vida y sus permisos desde la cuenta centralizada. Permites Cuentas de AWS que otros usen la clave, pero no permites otros permisos. Las cuentas externas no pueden administrar nada relacionado con el ciclo de vida de la clave ni con los permisos de acceso. Este modelo centralizado puede ayudar a minimizar el riesgo

de que los administradores o usuarios delegados eliminen las claves de forma no intencionada o aumenten sus privilegios.

La opción que elija depende de varios factores. Tenga en cuenta lo siguiente al elegir un enfoque:

1. ¿Tiene un proceso automatizado o manual para aprovisionar el acceso a las claves y los recursos? Esto incluye recursos como los procesos de implementación y las plantillas de infraestructura como código (IaC). Estas herramientas pueden ayudarlo a implementar y administrar recursos (como las claves de KMS, las políticas clave, las funciones de IAM y las políticas de IAM) en muchos casos. Cuentas de AWS Si no cuenta con estas herramientas de implementación, un enfoque centralizado de la administración de claves podría ser más fácil de administrar para su empresa.
2. ¿Tiene control administrativo sobre todos los recursos Cuentas de AWS que contienen claves de KMS? Si es así, un modelo centralizado puede simplificar la administración y eliminar la necesidad de cambiar Cuentas de AWS para administrar las claves. Sin embargo, tenga en cuenta que las funciones de IAM y los permisos de usuario para usar las claves aún deben administrarse por cuenta.
3. ¿Necesitas ofrecer acceso para usar tus claves de KMS a los clientes o socios que tengan sus propios Cuentas de AWS recursos? En el caso de estas claves, un enfoque centralizado puede reducir la carga administrativa de sus clientes y socios.
4. ¿Tiene requisitos de autorización para acceder a AWS los recursos que se resuelven mejor con un enfoque de acceso centralizado o local? Por ejemplo, si diferentes aplicaciones o unidades de negocio son responsables de administrar la seguridad de sus propios datos, es mejor adoptar un enfoque descentralizado de la administración de claves.
5. ¿Está excediendo las cuotas de recursos de servicio AWS KMS? Como estas cuotas se establecen por separado Cuenta de AWS, un modelo descentralizado distribuye la carga entre las cuentas, lo que multiplica de manera efectiva las cuotas de servicio.

> **Note**
>
> El modelo de administración de claves es irrelevante a la hora de considerar las cuotas de solicitud, ya que estas cuotas se aplican al director de la cuenta que hace una solicitud en relación con la clave, no a la cuenta que posee o administra la clave.

En general, le recomendamos que comience con un enfoque descentralizado, a menos que pueda explicar la necesidad de un modelo de claves KMS centralizado.

Elegir claves administradas por el cliente, claves AWS administradas o claves AWS propias

Las claves de KMS que crea y administra para usarlas en sus propias aplicaciones criptográficas se conocen como claves administradas por el cliente. Servicios de AWS puede usar claves administradas por el cliente para cifrar los datos que el servicio almacena en su nombre. Se recomiendan las claves administradas por el cliente si quieres tener un control total sobre el ciclo de vida y el uso de tus claves. Disponer de una clave administrada por el cliente en su cuenta tiene asociado un coste mensual. Además, las solicitudes de uso o administración de la clave conllevan un coste de uso. Para más información, consulte Precios de AWS KMS.

Si quiere cifrar sus datos, pero no quiere asumir los gastos generales o los costes que supone gestionar las claves, puede utilizar una clave AWS gestionada. Servicio de AWS Este tipo de clave existe en tu cuenta, pero solo se puede usar en determinadas circunstancias. Solo se puede usar en el contexto en el Servicio de AWS que operas y solo la pueden usar los directores de la cuenta que contiene la clave. No puedes gestionar nada relacionado con el ciclo de vida ni los permisos de estas claves. Algunas Servicios de AWS usan claves AWS administradas. El formato de un alias de clave AWS administrada es`aws/<service code>`. Por ejemplo, una `aws/ebs` clave solo se puede usar para cifrar los volúmenes de Amazon Elastic Block Store (Amazon EBS) en la misma cuenta que la clave y solo la pueden usar los directores de IAM de esa cuenta. Solo los usuarios de esa cuenta y para los recursos de esa cuenta pueden usar una clave AWS administrada. No puedes compartir recursos cifrados con una clave AWS gestionada con otras cuentas. Si esta es una limitación para su caso de uso, le recomendamos que utilice en su lugar una clave gestionada por el cliente; puede compartir el uso de esa clave con cualquier otra cuenta. No se te cobrará por la existencia de una clave AWS gestionada en tu cuenta, pero sí por cualquier uso de este tipo de clave por parte de la Servicio de AWS persona que esté asignada a la clave.

Una clave AWS gestionada es un tipo de clave heredada que dejará de crearse para nuevas a Servicios de AWS partir de 2021. En su lugar, las nuevas (y las antiguas) Servicios de AWS utilizan AWS una clave propia para cifrar los datos de forma predeterminada. AWS las claves propias son un conjunto de claves de KMS que una persona Servicio de AWS posee y administra para utilizarlas en múltiples Cuentas de AWS ocasiones. Si bien estas claves no están en sus manos Cuenta de AWS, Servicio de AWS puede usarlas para proteger los recursos de su cuenta.

Le recomendamos que utilice claves gestionadas por el cliente cuando lo más importante sea el control detallado y que utilice claves AWS propias cuando la comodidad sea lo más importante.

En la siguiente tabla se describen las principales diferencias de política, registro, administración y precios entre cada tipo de clave. Para obtener más información sobre los tipos de claves, consulte AWS KMS conceptos.

Consideración	Claves administradas por el cliente	AWS claves administradas	AWS claves propias
Política de claves	Controlada exclusivamente por el cliente	Controlada por el servicio; visible por el cliente	Controladas exclusivamente y solo visibles por quien Servicio de AWS cifra sus datos
Registro	AWS CloudTrail almacén de datos de eventos o registros de clientes	CloudTrail almacén de datos de eventos o seguimiento de clientes	No visible por el cliente
Gestión del ciclo de vida	El cliente gestiona la rotación, la eliminación y Región de AWS	Servicio de AWS gestiona la rotación (anual), la eliminación y la región	Servicio de AWS gestiona la rotación (anual), la eliminación y la región
Precios	Tarifa mensual por la existencia de la clave (prorrateada por hora); se cobra a la persona que llama por el uso de la API	La existencia de la clave es gratuita; se cobra a la persona que llama por el uso de la API	Sin cargos para el cliente

Elegir un almacén de AWS KMS claves

Un almacén de claves es un lugar seguro para almacenar y utilizar material de claves criptográficas. La mejor práctica del sector para los almacenes de claves es utilizar un dispositivo conocido como módulo de seguridad de hardware (HSM) que haya sido validado según el Programa de Validación de Módulos Criptográficos 140 de la Norma Federal de Procesamiento de Información (FIPS) del NIST con un nivel de seguridad 3. Existen otros programas para ayudar a los almacenes de llaves

que se utilizan para procesar los pagos. AWS Payment Cryptographyes un servicio que puede utilizar para proteger los datos relacionados con sus cargas de trabajo de pago.

AWS KMS admite varios tipos de almacenes de claves para ayudar a proteger el material de claves cuando se utiliza AWS KMS para crear y gestionar las claves de cifrado. Todas las opciones de almacenamiento de claves que ofrece se AWS KMS validan continuamente según la norma FIPS 140 en el nivel de seguridad 3. Están diseñados para evitar que cualquier persona, incluidos AWS los operadores, acceda a sus claves en texto plano o las utilice sin su permiso. Para obtener más información sobre los tipos de almacenes de claves disponibles, consulte los almacenes de claves en la AWS KMS documentación.

El almacén de claves AWS KMS estándar es la mejor opción para la mayoría de las cargas de trabajo. Si necesita elegir un tipo de almacén de claves diferente, considere detenidamente si los requisitos reglamentarios o de otro tipo (por ejemplo, internos) obligan a tomar esta decisión y evalúe cuidadosamente los costos y beneficios.

Eliminar y deshabilitar las claves de KMS

La eliminación de una clave KMS puede tener un impacto significativo. Antes de eliminar una clave de KMS que ya no vaya a utilizar, considere si es adecuado establecer el estado de la clave en Desactivado. Mientras una clave esté deshabilitada, no se puede usar para operaciones criptográficas. Todavía existe en AWS, y puede volver a habilitarlo en el futuro si es necesario. Las llaves deshabilitadas siguen incurriendo en gastos de almacenamiento. Le recomendamos que desactive las claves en lugar de eliminarlas hasta que esté seguro de que la clave no protege ningún dato o clave de datos.

> **Important**
>
> La eliminación de una clave debe planificarse cuidadosamente. Los datos no se pueden descifrar si se ha eliminado la clave correspondiente. AWS no tiene medios para recuperar una clave eliminada después de haberla eliminado. Al igual que con otras operaciones críticas AWS, debe aplicar una política que limite quién puede programar la eliminación de las claves y exija la autenticación multifactor (MFA) para la eliminación de las claves.

Para evitar la eliminación accidental de las claves, se AWS KMS aplica un período de espera mínimo predeterminado de siete días después de la ejecución de una `DeleteKey` llamada antes de que se elimine la clave. Puede establecer el período de espera en un valor máximo de 30 días. Durante el

período de espera, la clave sigue guardada AWS KMS en un estado de eliminación pendiente. No se puede utilizar para operaciones de cifrado o descifrado. Se registra cualquier intento de utilizar una clave que esté en estado de eliminación pendiente para el cifrado o el descifrado. AWS CloudTrail Puedes configurar una CloudWatch alarma de Amazon para estos eventos en tus CloudTrail registros. Si recibe alarmas sobre estos eventos, puede optar por cancelar el proceso de eliminación si es necesario. Hasta que el período de espera haya expirado, puede recuperar la clave del estado de eliminación pendiente y restaurarla al estado Desactivado o Activado.

Para eliminar una clave multiregional, es necesario eliminar las réplicas antes que la copia original. Para obtener más información, consulte Eliminar claves multirregionales.

Si utiliza una clave con material clave importado, puede eliminar el material clave importado inmediatamente. Esto es diferente de eliminar una clave de KMS en varios aspectos. Al realizar la `DeleteImportedKeyMaterial` acción, AWS KMS elimina el material clave y el estado de la clave cambia a Pendiente de importación. Tras eliminar el material clave, la clave queda inutilizable inmediatamente. No hay ningún período de espera. Para volver a permitir el uso de la clave, debe volver a importar el mismo material clave. El período de espera para eliminar las claves de KMS también se aplica a las claves de KMS con material de claves importado.

Si las claves de datos están protegidas por una clave de KMS y se utilizan activamente Servicios de AWS, no se ven afectadas de forma inmediata si la clave de KMS asociada está deshabilitada o si se elimina el material de clave importado. Por ejemplo, supongamos que se utilizó una clave con material importado para cifrar un objeto con SSE-KMS. Está cargando el objeto en un bucket de Amazon Simple Storage Service (Amazon S3). Antes de subir el objeto al depósito, debe importar el material a su clave. Una vez cargado el objeto, eliminas el material clave importado de esa clave. El objeto permanece en el depósito en un estado cifrado, pero nadie puede acceder al objeto hasta que el material clave eliminado se vuelva a importar a la clave. Si bien este flujo requiere una automatización precisa para importar y eliminar el material clave de una clave, puede proporcionar un nivel adicional de control dentro de un entorno.

AWS ofrece una guía prescriptiva para ayudarle a supervisar y corregir (si es necesario) la eliminación programada de las claves de KMS. Para obtener más información, consulte Supervisar y corregir la eliminación programada de claves. AWS KMS

Mejores prácticas de protección de datos para AWS KMS

Esta sección le ayuda a tomar decisiones sobre el uso de AWS Key Management Service (AWS KMS) claves para la protección de datos, por ejemplo, qué claves usar para cada tipo de datos. También proporciona ejemplos específicos del uso AWS KMS con diferentes Servicios de AWS. Estas recomendaciones y ejemplos le ayudan a comprender cuántas claves puede necesitar y qué entidades principales requieren permisos para utilizarlas.

En la sección también se analiza la rotación de claves. La rotación de claves es la práctica de reemplazar una clave KMS existente por una nueva clave o reemplazar el material criptográfico asociado a una clave KMS existente por material nuevo. Esta guía proporciona ejemplos e instrucciones sobre cómo rotar las claves de KMS para las de uso Servicios de AWS común. Las recomendaciones y los ejemplos están diseñados para ayudarle a tomar decisiones informadas sobre su estrategia de rotación clave.

Por último, en esta sección se ofrecen recomendaciones sobre cómo utilizar la AWS Encryption SDK herramienta para implementar el cifrado del lado del cliente en sus aplicaciones. En esta sección se incluyen las opciones de diseño que puede realizar en función del conjunto de funciones y las capacidades del. AWS Encryption SDK

En esta sección se tratan los siguientes temas de cifrado:

- Cifrado con AWS KMS
- Rotación clave AWS KMS y alcance del impacto
- Recomendaciones para usar el AWS Encryption SDK

Cifrado con AWS KMS

El cifrado es una práctica recomendada general para proteger la confidencialidad e integridad de la información confidencial. Debe utilizar los niveles de clasificación de datos existentes y tener al menos una AWS Key Management Service (AWS KMS) clave por nivel. Por ejemplo, puede definir una clave KMS para los datos clasificados como confidenciales, otra para los de uso interno y otra para los confidenciales. Esto le ayuda a asegurarse de que solo los usuarios autorizados tienen permisos para usar las claves asociadas a cada nivel de clasificación.

> **Note**
>
> Se puede usar una única clave KMS administrada por el cliente en cualquier combinación de aplicaciones Servicios de AWS o en sus propias aplicaciones que almacenen datos de una clasificación determinada. El factor que limita el uso de una clave en varias cargas de trabajo Servicios de AWS es la complejidad que deben tener los permisos de uso para controlar el acceso a los datos de un conjunto de usuarios. El documento JSON de la política AWS KMS clave debe tener menos de 32 KB. Si esta restricción de tamaño se convierte en una limitación, considere la posibilidad de utilizar AWS KMS concesiones o crear varias claves para minimizar el tamaño del documento de política clave.

En lugar de confiar únicamente en la clasificación de los datos para particionar la clave de KMS, también puede optar por asignar una clave de KMS para utilizarla en una clasificación de datos dentro de una sola Servicio de AWS. Por ejemplo, todos los datos etiquetados `Sensitive` en Amazon Simple Storage Service (Amazon S3) deben cifrarse con una clave de KMS que tenga un nombre similar. `S3-Sensitive` Además, puede distribuir sus datos entre varias claves de KMS dentro de la clasificación de datos Servicio de AWS o aplicación que haya definido. Por ejemplo, es posible que pueda eliminar algunos conjuntos de datos en un período de tiempo específico y eliminar otros conjuntos de datos en un período de tiempo diferente. Puede usar etiquetas de recursos para identificar y ordenar los datos cifrados con claves de KMS específicas.

Si elige un modelo de administración descentralizado para las claves de KMS, debe aplicar medidas de protección para garantizar la creación de nuevos recursos con una clasificación determinada y utilizar las claves de KMS esperadas con los permisos adecuados. Para obtener más información sobre cómo aplicar, detectar y administrar la configuración de los recursos mediante la automatización, consulte la Detección y monitoreo sección de esta guía.

En esta sección se analizan los siguientes temas de cifrado:

- Cifrado de datos de registro con AWS KMS
- Cifrado de forma predeterminada
- Cifrado de bases de datos AWS KMS
- Cifrado de datos PCI DSS con AWS KMS
- Uso de claves de KMS con Amazon EC2 Auto Scaling

Cifrado de datos de registro con AWS KMS

Muchos Servicios de AWS, como Amazon GuardDuty y AWS CloudTrail, ofrecen opciones para cifrar los datos de registro que se envían a Amazon S3. Al exportar los resultados desde GuardDuty Amazon S3, debe utilizar una clave de KMS. Le recomendamos que cifre todos los datos de registro y que conceda acceso a la desencriptación únicamente a los responsables autorizados, como los equipos de seguridad, el personal de respuesta a incidentes y los auditores.

La arquitectura AWS de referencia de seguridad recomienda crear una central para el registro. Cuenta de AWS Al hacerlo, también puede reducir la sobrecarga de administración de claves. Por ejemplo, con CloudTrail, puede crear un registro de la organización o un almacén de datos de eventos para registrar los eventos en toda su organización. Al configurar el registro organizativo o el almacén de datos de eventos, puede especificar un único bucket de Amazon S3 y una clave de KMS en la cuenta de registro designada. Esta configuración se aplica a todas las cuentas de los miembros de la organización. A continuación, todas las cuentas envían sus CloudTrail registros al bucket de Amazon S3 de la cuenta de registro y los datos de registro se cifran con la clave de KMS especificada. Debe actualizar la política de claves de esta clave de KMS para conceder CloudTrail los permisos necesarios para utilizarla. Para obtener más información, consulte Configurar las políticas AWS KMS clave CloudTrail en la CloudTrail documentación.

Para ayudar a proteger los CloudTrail registros GuardDuty y, el bucket de Amazon S3 y la clave de KMS deben estar en el mismo lugar Región de AWS. La arquitectura AWS de referencia de seguridad también proporciona orientación sobre las arquitecturas de registro y de cuentas múltiples. Al agregar registros de varias regiones y cuentas, consulta la sección Cómo crear un registro para una organización en la CloudTrail documentación para obtener más información sobre las regiones con las que se ha optado y asegurarte de que el registro centralizado funciona según lo diseñado.

Cifrado de forma predeterminada

Servicios de AWS Las que almacenan o procesan datos suelen ofrecer cifrado en reposo. Esta función de seguridad ayuda a proteger sus datos al cifrarlos cuando no están en uso. Los usuarios autorizados pueden seguir accediendo a ellos cuando lo necesiten.

Las opciones de implementación y cifrado varían entre sí Servicios de AWS. Muchas ofrecen cifrado de forma predeterminada. Es importante entender cómo funciona el cifrado para cada servicio que utilices. A continuación se muestran algunos ejemplos:

- Amazon Elastic Block Store (Amazon EBS): al habilitar el cifrado de forma predeterminada, se cifran todos los volúmenes y copias instantáneas nuevos de Amazon EBS. AWS Identity and

Access Management (IAM) o los usuarios no pueden lanzar instancias con volúmenes no cifrados o volúmenes que no admitan el cifrado. Esta función contribuye a la seguridad, el cumplimiento y la auditoría al garantizar que todos los datos almacenados en los volúmenes de Amazon EBS estén cifrados. Para obtener más información sobre el cifrado en este servicio, consulte el cifrado de Amazon EBS en la documentación de Amazon EBS.

- Amazon Simple Storage Service (Amazon S3): todos los objetos nuevos se cifran de forma predeterminada. Amazon S3 aplica automáticamente el cifrado del lado del servidor con claves administradas de Amazon S3 (SSE-S3) para cada objeto nuevo, a menos que especifique una opción de cifrado diferente. Los directores de IAM pueden seguir cargando objetos no cifrados en Amazon S3 indicándolo de forma explícita en la llamada a la API. En Amazon S3, para aplicar el cifrado SSE-KMS, debe usar una política de bucket con condiciones que requieran el cifrado. Para ver un ejemplo de política, consulte Requerir SSE-KMS para todos los objetos escritos en un bucket en la documentación de Amazon S3. Algunos buckets de Amazon S3 reciben y sirven una gran cantidad de objetos. Si esos objetos se cifran con claves de KMS, un gran número de operaciones de Amazon S3 se traduce en un gran número de `Decrypt` llamadas `GenerateDataKey` y llamadas a AWS KMS. Esto puede aumentar los cargos en los que incurra por su AWS KMS uso. Puede configurar las claves de bucket de Amazon S3, lo que puede reducir considerablemente sus AWS KMS costes. Para obtener más información sobre el cifrado en este servicio, consulte Protección de datos con cifrado en la documentación de Amazon S3.
- Amazon DynamoDB: DynamoDB es un servicio de base de datos NoSQL totalmente gestionado que permite el cifrado en reposo del lado del servidor de forma predeterminada y no se puede deshabilitar. Se recomienda utilizar una clave gestionada por el cliente para cifrar las tablas de DynamoDB. Este enfoque le ayuda a implementar los privilegios mínimos con permisos detallados y una separación de funciones al centrarse en usuarios y roles específicos de IAM en sus políticas clave. AWS KMS También puede elegir claves AWS administradas o AWS propias al configurar los ajustes de cifrado para las tablas de DynamoDB. Para los datos que requieren un alto grado de protección (donde los datos solo deben estar visibles como texto sin cifrar para el cliente), considere la posibilidad de utilizar el cifrado del lado del cliente con el SDK de cifrado de bases de datos.AWS Para obtener más información sobre el cifrado en este servicio, consulte Protección de datos en la documentación de DynamoDB.

Cifrado de bases de datos AWS KMS

El nivel en el que se implementa el cifrado afecta a la funcionalidad de la base de datos. Las ventajas y desventajas que debe tener en cuenta son las siguientes:

- Si solo utiliza el AWS KMS cifrado, el almacenamiento que respalda las tablas se cifra para DynamoDB y Amazon Relational Database Service (Amazon RDS). Esto significa que el sistema operativo que ejecuta la base de datos ve el contenido del almacenamiento como texto sin cifrar. Todas las funciones de la base de datos, incluida la generación de índices y otras funciones de orden superior que requieren acceso a los datos de texto sin formato, siguen funcionando según lo previsto.
- Amazon RDS se basa en cifrado de Amazon Elastic Block Store (Amazon EBS) para proporcionar cifrado de disco completo para los volúmenes de base de datos. Cuando crea una instancia de base de datos cifrada con Amazon RDS, Amazon RDS crea un volumen de Amazon EBS cifrado en su nombre para almacenar la base de datos. Los datos almacenados en reposo en el volumen, las instantáneas de la base de datos, las copias de seguridad automatizadas y las réplicas de lectura se cifran con la clave KMS que especificó al crear la instancia de base de datos.
- Amazon Redshift se integra AWS KMS y crea una jerarquía de claves de cuatro niveles que se utilizan para cifrar desde el nivel del clúster hasta el nivel de los datos. Al lanzar el clúster, puede optar por utilizar el cifrado. AWS KMS Solo la aplicación Amazon Redshift y los usuarios con los permisos adecuados pueden ver el texto sin cifrar al abrir (y descifrar) las tablas en la memoria. En términos generales, esto es análogo a las funciones de cifrado de datos transparente o basado en tablas (TDE) que están disponibles en algunas bases de datos comerciales. Esto significa que todas las funciones de la base de datos, incluidas las funciones de generación de índices y otras funciones de orden superior que requieren acceso a los datos de texto no cifrado, siguen funcionando según lo previsto.
- El cifrado a nivel de datos del lado del cliente implementado mediante el SDK de cifrado de AWS bases de datos (y herramientas similares) significa que tanto el sistema operativo como la base de datos solo ven el texto cifrado. Los usuarios solo pueden ver el texto sin formato si acceden a la base de datos desde un cliente que tenga instalado el SDK de cifrado de AWS bases de datos y tengan acceso a la clave correspondiente. Las funciones de bases de datos de orden superior que requieren acceso a texto sin formato para funcionar según lo previsto (como la generación de índices) no funcionarán si se indica que funcionan en campos cifrados. Si decide utilizar el cifrado del lado del cliente, asegúrese de utilizar un mecanismo de cifrado sólido que ayude a prevenir los ataques habituales contra los datos cifrados. Esto incluye el uso de un algoritmo de cifrado sólido y las técnicas adecuadas, como la sal, para ayudar a mitigar los ataques de texto cifrado.

Recomendamos utilizar las capacidades de cifrado AWS KMS integradas para los servicios de AWS bases de datos. En el caso de las cargas de trabajo que procesan datos confidenciales, se debe considerar el cifrado del lado del cliente para los campos de datos confidenciales. Al utilizar el cifrado

del lado del cliente, debe tener en cuenta el impacto en el acceso a la base de datos, como las uniones en consultas SQL o la creación de índices.

Cifrado de datos PCI DSS con AWS KMS

Los controles de seguridad y calidad se AWS KMS han validado y certificado para cumplir con los requisitos del estándar de seguridad de datos del sector de las tarjetas de pago (PCI DSS). Esto significa que puede cifrar los datos del número de cuenta principal (PAN) con una clave KMS. El uso de una clave KMS para cifrar datos elimina parte de la carga que supone administrar las bibliotecas de cifrado. Además, las claves KMS no se pueden exportar desde AWS KMS, lo que reduce la preocupación de que las claves de cifrado se almacenen de forma no segura.

Existen otras formas que puede utilizar AWS KMS para cumplir con los requisitos de PCI DSS. Por ejemplo, si lo utiliza AWS KMS con Amazon S3, puede almacenar datos PAN en Amazon S3 porque el mecanismo de control de acceso de cada servicio es distinto del otro.

Como siempre, al revisar sus requisitos de conformidad, asegúrese de obtener el asesoramiento de personas debidamente experimentadas, cualificadas y verificadas. Tenga en cuenta las cuotas de AWS KMS solicitud cuando diseñe aplicaciones que utilicen la clave directamente para proteger los datos de las transacciones con tarjetas incluidas en el ámbito de aplicación de la PCI DSS.

Como todas las AWS KMS solicitudes se registran AWS CloudTrail, puede auditar el uso de las claves revisando los CloudTrail registros. Sin embargo, si utiliza claves de bucket de Amazon S3, no habrá ninguna entrada que corresponda a cada acción de Amazon S3. Esto se debe a que la clave de bucket cifra las claves de datos que se utilizan para cifrar los objetos en Amazon S3. Si bien el uso de una clave de bucket no elimina todas las llamadas a la API AWS KMS, reduce su número. Como resultado, ya no hay one-to-one coincidencia entre los intentos de acceso a objetos de Amazon S3 y las llamadas a la API a AWS KMS.

Uso de claves de KMS con Amazon EC2 Auto Scaling

Amazon EC2 Auto Scaling es un servicio recomendado para automatizar el escalado de las EC2 instancias de Amazon. Le ayuda a asegurarse de que dispone del número correcto de instancias para gestionar la carga de su aplicación. Amazon EC2 Auto Scaling utiliza un rol vinculado a un servicio que proporciona los permisos adecuados al servicio y autoriza sus actividades en su cuenta. Para usar claves de KMS con Amazon EC2 Auto Scaling, sus políticas AWS KMS clave deben permitir que el rol vinculado al servicio utilice su clave de KMS con algunas operaciones de API, por ejemplo`Decrypt`, para que la automatización sea útil. Si la política AWS KMS clave no autoriza a la entidad principal de IAM que está realizando la operación a realizar una acción, dicha acción

será denegada. Para obtener más información sobre cómo aplicar correctamente los permisos en la política clave para permitir el acceso, consulte Protección de datos en Amazon EC2 Auto Scaling en la documentación de Amazon EC2 Auto Scaling.

Rotación clave AWS KMS y alcance del impacto

No recomendamos la rotación de claves AWS Key Management Service (AWS KMS), a menos que sea necesario rotar las claves por motivos de conformidad con la normativa. Por ejemplo, es posible que tengas que rotar tus claves de KMS debido a políticas empresariales, normas contractuales o normativas gubernamentales. El diseño reduce AWS KMS significativamente los tipos de riesgo que la rotación de claves suele utilizarse para mitigar. Si debe girar las claves KMS, le recomendamos que utilice la rotación de clave automática y la rotación de clave manual solo si no se admite la rotación automática de claves.

En esta sección se tratan los siguientes temas clave sobre la rotación:

- AWS KMS rotación clave simétrica
- Rotación de claves para los volúmenes de Amazon EBS
- Rotación de claves para Amazon RDS
- Rotación de claves para Amazon S3 y replicación en la misma región
- Rotación de claves KMS con material importado

AWS KMS rotación clave simétrica

AWS KMS admite la rotación automática de claves solo para claves KMS de cifrado simétrico con el material de clave que AWS KMS crea. La rotación automática es opcional para las claves KMS administradas por el cliente. Anualmente, AWS KMS rota el material clave de las claves de KMS AWS administradas. AWS KMS guarda todas las versiones anteriores del material criptográfico a perpetuidad, de modo que puede descifrar cualquier dato que esté cifrado con esa clave KMS. AWS KMS no elimina ningún material de clave girada hasta que elimine la clave KMS. Además, al descifrar un objeto mediante el uso AWS KMS, el servicio determina el material de soporte correcto que se debe utilizar en la operación de descifrado; no es necesario proporcionar parámetros de entrada adicionales.

Como AWS KMS conserva las versiones anteriores del material de claves criptográficas y se puede utilizar ese material para descifrar datos, la rotación de claves no ofrece ninguna ventaja de seguridad adicional. El mecanismo de rotación de claves existe para facilitar la rotación de claves si

se trabaja con una carga de trabajo en un contexto en el que lo exigen los requisitos reglamentarios o de otro tipo.

Rotación de claves para los volúmenes de Amazon EBS

Puede rotar las claves de datos de Amazon Elastic Block Store (Amazon EBS) mediante uno de los siguientes enfoques. El enfoque depende de los flujos de trabajo, los métodos de implementación y la arquitectura de la aplicación. Es posible que desee hacerlo al cambiar de una clave AWS administrada a una clave administrada por el cliente.

Utilizar las herramientas del sistema operativo para copiar los datos de un volumen a otro

1. Cree la nueva clave KMS. Para obtener instrucciones, consulte Crear una clave KMS.
2. Cree un nuevo volumen de Amazon EBS que sea del mismo tamaño o mayor que el original. Para el cifrado, especifique la clave KMS que creó. Para obtener instrucciones, consulte Crear un volumen de Amazon EBS.
3. Monte el nuevo volumen en la misma instancia o contenedor que el volumen original. Para obtener instrucciones, consulte Adjuntar un volumen de Amazon EBS a una EC2 instancia de Amazon.
4. Con la herramienta de sistema operativo que prefiera, copie los datos del volumen existente al nuevo volumen.
5. Cuando se complete la sincronización, durante un período de mantenimiento programado previamente, detenga el tráfico a la instancia. Para obtener instrucciones, consulta Cómo detener e iniciar las instancias manualmente.
6. Desmonte el volumen original. Para obtener instrucciones, consulte Separar un volumen de Amazon EBS de una instancia de Amazon EC2 .
7. Monte el nuevo volumen en el punto de montaje original.
8. Compruebe que el nuevo volumen funciona correctamente.
9. Elimine el volumen original. Para obtener instrucciones, consulte Eliminar un volumen de Amazon EBS.

Para usar una instantánea de Amazon EBS para copiar los datos de un volumen a otro

1. Cree la nueva clave KMS. Para obtener instrucciones, consulte Crear una clave KMS.
2. Cree una instantánea del volumen original en Amazon EBS. Para obtener instrucciones, consulte Crear instantáneas de Amazon EBS.

3. Cree un nuevo volumen a partir de la instantánea. Para el cifrado, especifique la nueva clave de KMS que creó. Para obtener instrucciones, consulte Crear un volumen de Amazon EBS.

   > **Note**
   >
   > En función de su carga de trabajo, es posible que desee utilizar la restauración rápida de instantáneas de Amazon EBS para minimizar la latencia inicial del volumen.

4. Crea una nueva EC2 instancia de Amazon. Para obtener instrucciones, consulta Lanzar una EC2 instancia de Amazon.
5. Adjunta el volumen que has creado a la EC2 instancia de Amazon. Para obtener instrucciones, consulte Adjuntar un volumen de Amazon EBS a una EC2 instancia de Amazon.
6. Transfiera la nueva instancia a producción.
7. Gire la instancia original para sacarla de producción y elimínela. Para obtener instrucciones, consulte Eliminar un volumen de Amazon EBS.

> **Note**
>
> Es posible copiar instantáneas y modificar la clave de cifrado utilizada para la copia de destino. Tras copiar la instantánea y cifrarla con las claves de KMS que prefieras, también puedes crear una Amazon Machine Image (AMI) a partir de las instantáneas. Para obtener más información, consulte el cifrado de Amazon EBS en la EC2 documentación de Amazon.

Rotación de claves para Amazon RDS

En el caso de algunos servicios, como Amazon Relational Database Service (Amazon RDS), el cifrado de datos se realiza dentro del servicio y lo proporciona. AWS KMS Siga las instrucciones siguientes para rotar una clave de una instancia de base de datos de Amazon RDS.

Para rotar una clave de KMS para una base de datos de Amazon RDS

1. Cree una instantánea de la base de datos cifrada original. Para obtener instrucciones, consulte Administrar copias de seguridad manuales en la documentación de Amazon RDS.
2. Copie la instantánea en una nueva instantánea. Para el cifrado, especifique la nueva clave KMS. Para obtener instrucciones, consulte Copiar una instantánea de base de datos para Amazon RDS.

3. Utilice la nueva instantánea para crear un nuevo clúster de Amazon RDS. Para obtener instrucciones, consulte Restauración en una instancia de base de datos en la documentación de Amazon RDS. De forma predeterminada, el clúster usa la nueva clave de KMS.
4. Compruebe el funcionamiento de la nueva base de datos y los datos que contiene.
5. Pase la nueva base de datos a producción.
6. Haga que la base de datos antigua deje de estar en producción y elimínela. Para obtener instrucciones, consulte Eliminar una instancia de base de datos.

Rotación de claves para Amazon S3 y replicación en la misma región

En el caso de Amazon Simple Storage Service (Amazon S3), para cambiar la clave de cifrado de un objeto, debe leer y volver a escribir el objeto. Al reescribir el objeto, se especifica de forma explícita la nueva clave de cifrado en la operación de escritura. Para hacer esto con muchos objetos, puede utilizar Amazon S3 Batch Operations. En la configuración del trabajo, especifique la nueva configuración de cifrado para la operación de copia. Por ejemplo, puede elegir SSE-KMS e introducir el KeyID.

Como alternativa, puede usar Amazon S3 Same Region Replication (SRR). SSR puede volver a cifrar los objetos en tránsito.

Rotación de claves KMS con material importado

AWS KMS no recupera ni rota el material clave importado. Para girar una clave KMS con material clave importado, debe girar la clave manualmente.

Recomendaciones para usar el AWS Encryption SDK

AWS Encryption SDKEs una herramienta poderosa para implementar el cifrado del lado del cliente en sus aplicaciones. Hay bibliotecas disponibles para Java JavaScript, C, Python y otros lenguajes de programación. Se integra con AWS Key Management Service (AWS KMS). También puede usarlo como un SDK independiente sin hacer referencia a las claves de KMS.

Las prácticas recomendadas para utilizar esta herramienta incluyen considerar detenidamente los requisitos de la aplicación. Equilibre esos requisitos con los riesgos que pueden presentar determinadas configuraciones, como la introducción del almacenamiento en caché de claves en su aplicación. Para obtener más información sobre el almacenamiento en caché de claves de datos, consulte Almacenamiento en caché de claves de datos en la documentación. AWS Encryption SDK

Tenga en cuenta las siguientes preguntas a la hora de decidir si se debe utilizar: AWS Encryption SDK

- ¿Existe algún requisito de cifrado del lado del cliente que no pueda cumplirse con el cifrado del lado del servidor con servicios que se integren? AWS KMS
- ¿Puede proteger adecuadamente las claves que se utilizan para cifrar los datos en el lado del cliente y cómo lo hará?
- ¿Existen otras bibliotecas de fit-for-purpose cifrado que se adapten mejor a su caso de uso? Considere AWS ofertas alternativas, como el cifrado del lado del cliente de Amazon S3 y el SDK de cifrado de AWS bases de datos.

Para obtener más información sobre cómo elegir el servicio adecuado para su caso de uso, consulte la documentación de AWS Crypto Tools.

Mejores prácticas de gestión de identidades y accesos para AWS KMS

Para usar AWS Key Management Service (AWS KMS), debe tener credenciales que AWS pueda usar para autenticar y autorizar sus solicitudes. Ningún AWS director tiene permisos para acceder a una clave de KMS a menos que dicho permiso se otorgue de forma explícita y nunca se deniegue. No hay permisos implícitos o automáticos para usar o administrar una clave de KMS. En los temas de esta sección se definen las prácticas recomendadas de seguridad para ayudarle a determinar qué controles de administración de AWS KMS acceso debe utilizar para proteger su infraestructura.

En esta sección se analizan los siguientes temas de administración de identidades y accesos:

- AWS KMS políticas clave y políticas de IAM
- Permisos con privilegios mínimos para AWS KMS
- Control de acceso basado en roles para AWS KMS
- Control de acceso basado en atributos para AWS KMS
- Contexto de cifrado para AWS KMS
- Solución de problemas de AWS KMS permisos

AWS KMS políticas clave y políticas de IAM

La forma principal de gestionar el acceso a AWS KMS los recursos es mediante políticas. Las políticas son documentos que describen qué entidades principales pueden acceder a qué recursos. Las políticas asociadas a una identidad AWS Identity and Access Management (IAM) (usuarios, grupos de usuarios o funciones) se denominan políticas basadas en la identidad. Las políticas de IAM que se asocian a los recursos se denominan políticas basadas en recursos. AWS KMS las políticas de recursos para las claves de KMS se denominan políticas clave. Además de las políticas de IAM y las políticas AWS KMS clave, AWS KMS apoya las subvenciones. Las concesiones proporcionan una forma flexible y eficaz de delegar permisos. Puede utilizar las subvenciones para conceder claves de acceso KMS con un límite de tiempo limitado a los directores de IAM en su Cuenta de AWS país o en otros países. Cuentas de AWS

Todas las claves KMS tienen una política de claves. Si no proporciona una, AWS KMS crea una para usted. La política de claves predeterminada que se AWS KMS utiliza varía en función de si se crea la clave mediante la AWS KMS consola o si se utiliza la AWS KMS API. Le recomendamos que edite

la política de claves predeterminada para adaptarla a los requisitos de su organización en materia de permisos con privilegios mínimos. Esto también debería ajustarse a su estrategia de uso de las políticas de IAM junto con las políticas clave. Para obtener más recomendaciones sobre el uso de las políticas de IAM con AWS KMS, consulte las prácticas recomendadas para las políticas de IAM en la documentación. AWS KMS

Puede utilizar la política clave para delegar la autorización de un director de IAM en la política basada en la identidad. También puede usar la política clave para refinar la autorización junto con la política basada en la identidad. En cualquier caso, tanto la política clave como la política basada en la identidad determinan el acceso, junto con cualquier otra política aplicable que abarque el acceso, como las políticas de control de servicios (), las políticas de control de recursos (SCPs)o los límites de los RCPs permisos. Si el principal está en una cuenta diferente a la clave de KMS, básicamente, solo se admiten las acciones criptográficas y de concesión. Para obtener más información sobre este escenario de cuentas múltiples, consulte Permitir que los usuarios de otras cuentas usen una clave KMS en la AWS KMS documentación.

Debe usar políticas de IAM basadas en la identidad en combinación con políticas clave para controlar el acceso a sus claves de KMS. Las subvenciones también se pueden utilizar en combinación con estas políticas para controlar el acceso a una clave de KMS. Para utilizar una política basada en la identidad para controlar el acceso a una clave de KMS, la política de claves debe permitir que la cuenta utilice políticas basadas en la identidad. Puede especificar una declaración de política de claves que habilite las políticas de IAM o puede especificar explícitamente la entidad principal permitida en la política de claves.

Al redactar políticas, asegúrese de contar con controles estrictos que restrinjan quién puede realizar las siguientes acciones:

- Actualice, cree y elimine las políticas de IAM y las políticas clave de KMS
- Adjunte y separe las políticas basadas en la identidad de los usuarios, roles y grupos
- Adjunte y separe las políticas clave de las AWS KMS claves de KMS
- Cree concesiones para sus claves de KMS: ya sea que controle el acceso a sus claves de KMS exclusivamente con políticas clave o que combine las políticas clave con las políticas de IAM, debe restringir la capacidad de modificar las políticas. Implemente un proceso de aprobación para cambiar cualquier política existente. Un proceso de aprobación puede ayudar a evitar lo siguiente:
  - Pérdida accidental de los permisos principales de IAM: es posible realizar cambios que impidan que los responsables de IAM puedan gestionar la clave o utilizarla en operaciones criptográficas. En situaciones extremas, es posible revocar los permisos de administración de claves de

todos los usuarios. Si esto ocurre, debes ponerte en contacto con nosotros AWS Supportpara recuperar el acceso a la clave.

- Cambios no aprobados en las políticas clave de KMS: si un usuario no autorizado obtiene acceso a la política clave, podría modificarla para delegar los permisos a una persona no autorizada Cuenta de AWS o principal.
- Cambios no aprobados en las políticas de IAM: si un usuario no autorizado obtiene un conjunto de credenciales con permisos para administrar la membresía de un grupo, podría aumentar sus propios permisos y realizar cambios en sus políticas de IAM, políticas clave, configuración de claves de KMS u otras configuraciones de recursos. AWS

Revise detenidamente las funciones y los usuarios de IAM asociados a los directores de IAM designados como sus administradores clave de KMS. Esto puede ayudar a evitar eliminaciones o cambios no autorizados. Si necesita cambiar los principales que tienen acceso a sus claves de KMS, compruebe que los nuevos directores de administrador se agreguen a todas las políticas clave obligatorias. Pruebe sus permisos antes de eliminar el principal administrador anterior. Recomendamos encarecidamente seguir todas las prácticas recomendadas de seguridad de IAM y utilizar credenciales temporales en lugar de credenciales de larga duración.

Te recomendamos conceder permisos de acceso con plazos determinados mediante subvenciones si no conoces los nombres de los directores en el momento de crear las políticas o si los directores que requieren acceso cambian con frecuencia. El principal beneficiario puede estar en la misma cuenta que la clave de KMS o en una cuenta diferente. Si la clave principal y la clave de KMS están en cuentas diferentes, debe especificar una política basada en la identidad además de la concesión. Las concesiones requieren una administración adicional, ya que debe llamar a una API para crear la concesión y para retirarla o revocarla cuando ya no sea necesaria.

Ningún responsable AWS , ni siquiera el usuario raíz de la cuenta o el creador de la clave, tiene permisos para acceder a una clave de KMS, a menos que se les permita de forma explícita y no se les deniegue explícitamente en una política de claves, una política de IAM o una concesión. Por extensión, debes tener en cuenta qué pasaría si un usuario obtuviera acceso no deseado para usar una clave de KMS y cuál sería el impacto. Para mitigar este riesgo, tenga en cuenta lo siguiente:

- Puede mantener diferentes claves de KMS para diferentes categorías de datos. Esto le ayuda a separar las claves y a mantener políticas clave más concisas que contienen declaraciones de políticas que se refieren específicamente al acceso principal a esa categoría de datos. También significa que, si se accede a las credenciales de IAM pertinentes de forma no intencionada, la

identidad vinculada a ese acceso solo tendrá acceso a las claves especificadas en la política de IAM y solo si la política de claves permite el acceso a ese principal.

- Puede evaluar si un usuario con acceso no deseado a la clave puede acceder a los datos. Por ejemplo, con Amazon Simple Storage Service (Amazon S3), el usuario también debe tener los permisos adecuados para acceder a los objetos cifrados en Amazon S3. Como alternativa, si un usuario tiene acceso no deseado (mediante RDP o SSH) a una EC2 instancia de Amazon que tiene un volumen cifrado con una clave de KMS, el usuario puede acceder a los datos mediante las herramientas del sistema operativo.

> **Note**
>
> Servicios de AWS ese uso AWS KMS no expone el texto cifrado a los usuarios (la mayoría de los enfoques actuales de criptoanálisis requieren el acceso al texto cifrado). Además, el texto cifrado no está disponible para su examen físico fuera de un centro de AWS datos porque todos los soportes de almacenamiento se destruyen físicamente cuando se retiran del servicio, de acuerdo con los requisitos del NIST 00-88. SP8

Permisos con privilegios mínimos para AWS KMS

Dado que sus claves KMS protegen la información confidencial, le recomendamos que siga el principio del acceso con menos privilegios. Cuando defina las políticas de claves, delegue los permisos mínimos necesarios para realizar una tarea. Permita todas las acciones (`kms:*`) de una política de claves de KMS solo si planea restringir aún más los permisos con políticas adicionales basadas en la identidad. Si planea administrar los permisos con políticas basadas en la identidad, limite quién tiene la capacidad de crear y adjuntar políticas de IAM a las entidades principales de IAM y supervise los cambios en las políticas.

Si permites todas las acciones (`kms:*`) tanto en la política clave como en la política basada en la identidad, el responsable tiene permisos administrativos y de uso para la clave de KMS. Como práctica recomendada de seguridad, recomendamos delegar estos permisos únicamente a directores específicos. Considere cómo asignar los permisos a los directores que administrarán sus claves y a los principales que usarán sus claves. Puede hacerlo nombrando explícitamente al principal en la política de claves o limitando a qué principios se asocia la política basada en la identidad. También puede usar claves de condición para restringir los permisos. Por ejemplo, puedes usar aws:

PrincipalTag para permitir todas las acciones si el director que realiza la llamada a la API tiene la etiqueta especificada en la regla de condición.

Para entender cómo se evalúan las declaraciones de políticas AWS, consulte la lógica de evaluación de políticas en la documentación de IAM. Recomendamos revisar este tema antes de redactar políticas para ayudar a reducir la posibilidad de que su política tenga efectos no deseados, como proporcionar acceso a directores que no deberían tener acceso.

> **Tip**
>
> Cuando pruebe una aplicación en un entorno que no sea de producción, utilice AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) como ayuda para aplicar los permisos con privilegios mínimos en sus políticas de IAM.

Si utiliza usuarios de IAM en lugar de funciones de IAM, le recomendamos encarecidamente que utilice la autenticación AWS multifactor (MFA) para mitigar la vulnerabilidad de las credenciales a largo plazo. Puede utilizar la MFA para hacer lo siguiente:

- Requerir que los usuarios validen sus credenciales con MFA antes de realizar acciones privilegiadas, como programar la eliminación de claves.
- Dividir la propiedad de una contraseña de cuenta de administrador y el dispositivo de MFA entre varias personas para implementar la autorización dividida.

Para ver ejemplos de políticas que pueden ayudarle a configurar los permisos con privilegios mínimos, consulte los ejemplos de políticas de IAM en la documentación. AWS KMS

Control de acceso basado en roles para AWS KMS

El control de acceso basado en roles (RBAC) es una estrategia de autorización que proporciona a los usuarios solo los permisos necesarios para realizar sus tareas laborales, y nada más. Es un enfoque que puede ayudarlo a implementar el principio del privilegio mínimo.

AWS KMS es compatible con RBAC. Le permite controlar el acceso a sus claves especificando permisos detallados dentro de las políticas clave. Las políticas de claves especifican un recurso, una acción, un efecto, una entidad principal y unas condiciones opcionales para conceder el acceso a las claves. Para implementar el RBAC en AWS KMS, recomendamos separar los permisos de los usuarios clave de los administradores clave.

Para los usuarios clave, asigne solo los permisos que el usuario necesite. Usa las siguientes preguntas para ayudarte a refinar aún más los permisos:

- ¿Qué directores de IAM necesitan acceder a la clave?
- ¿Qué acciones debe realizar cada entidad principal con la clave? Por ejemplo, ¿el director solo necesita permisos`Encrypt`? `Sign`
- ¿A qué recursos necesita acceder el director?
- ¿La entidad es un ser humano o un Servicio de AWS? Si se trata de un servicio, puedes usar la clave kms: ViaService condition para restringir el uso de la clave a un servicio específico.

En el caso de los administradores clave, asigne solo los permisos que el administrador necesite. Por ejemplo, los permisos de un administrador pueden variar en función de si la clave se utiliza en entornos de prueba o de producción. Si utiliza permisos menos restrictivos en determinados entornos que no son de producción, implemente un proceso para probar las políticas antes de ponerlas en producción.

Para ver ejemplos de políticas que pueden ayudarle a configurar el control de acceso basado en roles para los principales usuarios y administradores, consulte RBAC para. AWS KMS

Control de acceso basado en atributos para AWS KMS

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos. Al igual que el RBAC, es un enfoque que puede ayudarlo a implementar el principio del privilegio mínimo.

AWS KMS es compatible con ABAC, ya que permite definir los permisos en función de las etiquetas asociadas al recurso de destino, como una clave de KMS, y de las etiquetas asociadas a la persona que realiza la llamada a la API. En AWS KMS, puedes usar etiquetas y alias para controlar el acceso a las claves gestionadas por tus clientes. Por ejemplo, puede definir políticas de IAM que utilicen claves de condición de etiqueta para permitir operaciones cuando la etiqueta del principal coincida con la etiqueta asociada a la clave de KMS. Para ver un tutorial, consulte Definir los permisos de acceso a AWS los recursos en función de las etiquetas en la AWS KMS documentación.

Como práctica recomendada, utilice las estrategias de ABAC para simplificar la gestión de las políticas de IAM. Con ABAC, los administradores pueden usar etiquetas para permitir el acceso a nuevos recursos en lugar de actualizar las políticas existentes. ABAC requiere menos políticas porque no es necesario crear políticas diferentes para diferentes funciones laborales. Para

obtener más información, consulte Comparación del ABAC con el modelo RBAC tradicional en la documentación de IAM.

Aplique la mejor práctica de permisos con privilegios mínimos al modelo ABAC. Proporcione a los directores de IAM solo los permisos que necesitan para realizar sus tareas. Controle cuidadosamente el acceso al etiquetado para APIs que los usuarios puedan modificar las etiquetas de las funciones y los recursos. Si utilizas claves de condición de alias clave como soporte para ABAC AWS KMS, asegúrate de disponer también de controles estrictos que restrinjan quién puede crear claves y modificar los alias.

También puedes usar etiquetas para vincular una clave específica a una categoría empresarial y comprobar que se está utilizando la clave correcta para una acción determinada. Por ejemplo, puedes usar AWS CloudTrail los registros para comprobar que la clave utilizada para realizar una AWS KMS acción específica pertenece a la misma categoría empresarial que el recurso en el que se está utilizando.

> **Warning**
>
> No incluya información confidencial en la clave ni en el valor de la etiqueta. Las etiquetas no están cifradas. Son accesibles para muchos Servicios de AWS, incluida la facturación.

Antes de implementar un enfoque ABAC en su control de acceso, considere si los demás servicios que utiliza admiten este enfoque. Si necesita ayuda para determinar qué servicios son compatibles con ABAC, consulte quéServicios de AWS servicios funcionan con IAM en la documentación de IAM.

Para obtener más información sobre la implementación de ABAC AWS KMS y las claves de condiciones que pueden ayudarle a configurar las políticas, consulte ABAC for. AWS KMS

Contexto de cifrado para AWS KMS

Todas las operaciones AWS KMS criptográficas con claves KMS de cifrado simétrico aceptan un contexto de cifrado. El contexto de cifrado es un conjunto opcional de pares clave-valor no secretos que pueden contener información contextual adicional sobre los datos. Como práctica recomendada, puede insertar el contexto de cifrado en `Encrypt` las operaciones AWS KMS para mejorar la autorización y la auditabilidad de las llamadas a la API de descifrado. AWS KMS AWS KMS utiliza el contexto de cifrado como datos autenticados adicionales (AAD) para respaldar el cifrado autenticado. El contexto de cifrado se vincula criptográficamente al texto cifrado, de tal forma que se requiera el mismo contexto de cifrado para descifrar los datos.

El contexto de cifrado no es secreto y no está cifrado. Aparece en texto plano en AWS CloudTrail los registros para que pueda usarlo para identificar y clasificar sus operaciones criptográficas. Como el contexto de cifrado no es secreto, debe permitir que solo las personas autorizadas accedan a sus datos de registro. CloudTrail

También puede usar las EncryptionContextKeys claves condicionales kms ::context-key EncryptionContext y kms: para controlar el acceso a una clave KMS de cifrado simétrico en función del contexto de cifrado. También puede usar estas claves de condición para exigir que los contextos de cifrado se utilicen en las operaciones criptográficas. Para estas claves de condición, consulte las instrucciones sobre el uso `ForAnyValue` o `ForAllValues` configuración de operadores para asegurarse de que sus políticas reflejen los permisos previstos.

Solución de problemas de AWS KMS permisos

Cuando redacte políticas de control de acceso para una clave de KMS, tenga en cuenta cómo funcionan juntas la política de IAM y la política clave. Los permisos efectivos de un principal son los permisos que todas las políticas vigentes conceden (y no deniegan de forma explícita). Dentro de una cuenta, los permisos de una clave de KMS pueden verse afectados por las políticas de IAM basadas en la identidad, las políticas clave, los límites de los permisos, las políticas de control de servicios o las políticas de sesión. Por ejemplo, si utilizas políticas clave y basadas en la identidad para controlar el acceso a la clave de KMS, se evalúan todas las políticas relacionadas con el principal y el recurso para determinar la autorización del principal para realizar una acción determinada. Para obtener más información, consulte Lógica de evaluación de políticas en la documentación de IAM.

Para obtener información detallada y un diagrama de flujo para solucionar problemas de acceso a claves, consulte Solución de problemas de acceso a claves en la documentación. AWS KMS

Para solucionar un mensaje de error de acceso denegado

1. Confirme que las políticas basadas en la identidad de IAM y las políticas clave de KMS permiten el acceso.
2. Confirme que un límite de permisos en IAM no restrinja el acceso.
3. Confirme que una política de control de servicios (SCP) o una política de control de recursos (RCP) no restrinja AWS Organizations el acceso.
4. Si utiliza puntos de enlace de VPC, confirme que las políticas de puntos de enlace sean correctas.

5. En las políticas basadas en la identidad y en las políticas clave, elimine cualquier condición o referencia a recursos que restrinja el acceso a la clave. Tras eliminar estas restricciones, confirme que el director puede llamar correctamente a la API en la que se produjo el error anterior. Si tiene éxito, vuelva a aplicar las condiciones y las referencias a los recursos una por una y, después de cada una, compruebe que el principal sigue teniendo acceso. Esto le ayuda a identificar la condición o la referencia de recurso que está causando el error.

Para obtener más información, consulte Solución de problemas de mensajes de error de acceso denegado en la documentación de IAM.

Mejores prácticas de detección y monitoreo para AWS KMS

La detección y el monitoreo son una parte importante para comprender la disponibilidad, el estado y el uso de sus AWS Key Management Service (AWS KMS) claves. La supervisión ayuda a mantener la seguridad, la confiabilidad, la disponibilidad y el rendimiento de sus AWS soluciones. AWS proporciona varias herramientas para monitorear sus claves y AWS KMS operaciones de KMS. En esta sección, se describe cómo configurar y utilizar estas herramientas para obtener una mayor visibilidad del entorno y supervisar el uso de las claves de KMS.

En esta sección se analizan los siguientes temas de detección y supervisión:

- Supervise AWS KMS las operaciones con AWS CloudTrail
- Supervisión del acceso a las claves de KMS con IAM Access Analyzer
- Monitorear la configuración de cifrado de otros Servicios de AWS con AWS Config
- Supervisión de claves KMS con CloudWatch alarmas de Amazon
- Automatizar las respuestas con Amazon EventBridge

Supervise AWS KMS las operaciones con AWS CloudTrail

AWS KMS está integrado con AWS CloudTrailun servicio que puede grabar todas las llamadas realizadas AWS KMS por los usuarios, los roles y otros Servicios de AWS. CloudTrail captura todas las llamadas a la API AWS KMS como eventos, incluidas las llamadas desde la AWS KMS consola AWS KMS APIs AWS CloudFormation,,, AWS Command Line Interface (AWS CLI) y Herramientas de AWS para PowerShell.

CloudTrail registra todas AWS KMS las operaciones, incluidas las de solo lectura, como `ListAliases` y. `GetKeyRotationStatus` También registra las operaciones que administran las claves de KMS, como `CreateKey` y`PutKeyPolicy, and cryptographic operations, such as GenerateDataKey`. `Decrypt` También registra las operaciones internas AWS KMS que lo requieran, como`DeleteExpiredKeyMaterial`, `DeleteKeySynchronizeMultiRegionKey`, y`RotateKey`.

CloudTrail está activado Cuenta de AWS cuando lo crea. De forma predeterminada, el historial de eventos proporciona un registro visible, consultable, descargable e inmutable de los últimos 90 días de actividad registrada en la API de eventos de gestión en un. Región de AWSPara supervisar o auditar el uso de tus claves de KMS más allá de los 90 días, te recomendamos crear un registro para ti. CloudTrail Cuenta de AWS Si ha creado una organización en AWS Organizations, puede crear un

registro de la organización o un almacén de datos de eventos que registre los eventos de todos los Cuentas de AWS miembros de esa organización.

Una vez que hayas establecido un registro para tu cuenta u organización, puedes usar otro Servicios de AWS para almacenar, analizar y responder automáticamente a los eventos que se registran en el registro. Por ejemplo, puede hacer lo siguiente:

- Puedes configurar CloudWatch alarmas de Amazon que te notifiquen ciertos eventos en la ruta. Para obtener más información, consulte la sección Supervisión de claves KMS con CloudWatch alarmas de Amazon de esta guía.
- Puedes crear EventBridge reglas de Amazon que realicen automáticamente una acción cuando se produzca un evento en la ruta. Para obtener más información, consulta Automatizar las respuestas con Amazon EventBridge en esta guía.
- Puede usar Amazon Security Lake para recopilar y almacenar registros de varios Servicios de AWS, incluidos CloudTrail. Para obtener más información, consulte Recopilación de datos desde Servicios de AWS Security Lake en la documentación de Amazon Security Lake.
- Para mejorar el análisis de la actividad operativa, puede consultar CloudTrail los registros con Amazon Athena. Para obtener más información, consulte AWS CloudTrail los registros de consultas en la documentación de Amazon Athena.

Para obtener más información sobre cómo monitorear AWS KMS las operaciones con CloudTrail, consulte lo siguiente:

- Registrar llamadas a la AWS KMS API con AWS CloudTrail
- Ejemplos de entradas de AWS KMS registro
- Supervise las claves de KMS con Amazon EventBridge
- CloudTrail integración con Amazon EventBridge

Supervisión del acceso a las claves de KMS con IAM Access Analyzer

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) le ayuda a identificar los recursos de su organización y las cuentas (como las claves de KMS) que se comparten con una entidad externa. Este servicio puede ayudarlo a identificar el acceso no intencionado o demasiado amplio a sus recursos y datos, lo que constituye un riesgo para la seguridad. IAM Access Analyzer

identifica los recursos que se comparten con entidades externas mediante un razonamiento basado en la lógica para analizar las políticas basadas en los recursos de su entorno. AWS

Puede utilizar IAM Access Analyzer para identificar qué entidades externas tienen acceso a sus claves de KMS. Al activar IAM Access Analyzer, se crea un analizador para toda la organización o para una cuenta de destino. La organización o cuenta que elija se conoce como zona de confianza del analizador. El analizador supervisa los recursos compatibles dentro de la zona de confianza. Cualquier acceso a los recursos por parte de los directores dentro de la zona de confianza se considera de confianza.

En el caso de las claves KMS, IAM Access Analyzer analiza las políticas y concesiones clave que se aplican a una clave. Determina si una política o concesión clave permite a una entidad externa acceder a la clave. Utilice el analizador de acceso de IAM para determinar si las entidades externas tienen acceso a sus claves de KMS y, a continuación, compruebe si esas entidades deberían tener acceso.

Para obtener más información sobre el uso del analizador de acceso de IAM para supervisar el acceso a las claves de KMS, consulte lo siguiente:

- Uso de AWS Identity and Access Management Access Analyzer
- Tipos de recursos de IAM Access Analyzer para acceso externo
- Tipos de recursos de IAM Access Analyzer: AWS KMS keys
- Hallazgos relacionados con el acceso externo y no utilizado

Monitorear la configuración de cifrado de otros Servicios de AWS con AWS Config

AWS Configproporciona una vista detallada de la configuración de AWS los recursos de su Cuenta de AWS. Puede utilizarlo AWS Config para comprobar que los Servicios de AWS que utilizan sus claves de KMS tienen sus ajustes de cifrado configurados adecuadamente. Por ejemplo, puede usar la AWS Config regla de volúmenes cifrados para validar que los volúmenes de Amazon Elastic Block Store (Amazon EBS) estén cifrados.

AWS Config incluye reglas administradas que le ayudan a elegir rápidamente las reglas con las que evaluar sus recursos. Compruebe AWS Config si las reglas gestionadas que necesita son compatibles en esa región. Regiones de AWS Las reglas gestionadas disponibles incluyen las comprobaciones de configuración de las instantáneas del Amazon Relational Database Service

(Amazon RDS), el cifrado de pistas CloudTrail , el cifrado predeterminado para los depósitos de Amazon Simple Storage Service (Amazon S3), el cifrado de tablas de Amazon DynamoDB y mucho más.

También puede crear reglas personalizadas y aplicar su lógica empresarial para determinar si sus recursos cumplen con sus requisitos. El código fuente abierto de muchas reglas administradas está disponible en el repositorio de AWS Config reglas en GitHub. Pueden ser un punto de partida útil para desarrollar tus propias reglas personalizadas.

Cuando un recurso no cumple con una regla, puede iniciar acciones de respuesta. AWS Config incluye las acciones de corrección que lleva a cabo AWS Systems Manager Automation. Por ejemplo, si ha aplicado la cloud-trail-encryption-enabledregla y la regla arroja un `NON_COMPLIANT` resultado, AWS Config puede iniciar un documento de automatización que solucione el problema cifrando los CloudTrail registros por usted.

AWS Config le permite comprobar de forma proactiva el cumplimiento de AWS Config las reglas antes de aprovisionar los recursos. La aplicación de reglas en modo proactivo le ayuda a evaluar las configuraciones de los recursos de la nube antes de crearlos o actualizarlos. La aplicación de reglas en modo proactivo como parte de su proceso de implementación le permite probar las configuraciones de los recursos antes de desplegarlos.

También puede implementar AWS Config reglas como controles AWS Security Hub. Security Hub ofrece estándares de seguridad que puede aplicar a su Cuentas de AWS. Estos estándares le ayudan a evaluar su entorno en función de las prácticas recomendadas. El estándar de prácticas recomendadas de seguridad AWS fundamentales incluye controles dentro de la categoría de control de protección para comprobar que el cifrado en reposo está configurado y que las políticas de claves de KMS siguen las prácticas recomendadas.

Para obtener más información sobre AWS Config cómo supervisar la configuración de cifrado en Servicios de AWS, consulte lo siguiente:

- Introducción a AWS Config
- AWS Config reglas gestionadas
- AWS Config reglas personalizadas
- Corregir los recursos no conformes con AWS Config

Supervisión de claves KMS con CloudWatch alarmas de Amazon

Amazon CloudWatch supervisa tus AWS recursos y las aplicaciones en las que ejecutas AWS en tiempo real. Puede utilizarlas CloudWatch para recopilar y realizar un seguimiento de las métricas, que son variables que puede medir.

La caducidad del material clave importado, o la eliminación de una clave, son eventos potencialmente catastróficos si no son intencionados o no se planifican adecuadamente. Le recomendamos que configure CloudWatch las alarmas para que le avisen de estos eventos antes de que se produzcan. También le recomendamos que configure políticas AWS Identity and Access Management (de IAM) o políticas de control de AWS Organizations servicios (SCPs) para evitar la eliminación de claves importantes.

CloudWatch las alarmas le ayudan a tomar medidas correctivas, como cancelar la eliminación de claves, o tomar medidas correctivas, como volver a importar el material clave eliminado o caducado.

Automatizar las respuestas con Amazon EventBridge

También puede usar Amazon EventBridge para notificarle eventos importantes que afecten a sus claves de KMS. EventBridge es una Servicio de AWS que ofrece un flujo casi en tiempo real de los eventos del sistema que describen los cambios en los AWS recursos. EventBridgerecibe automáticamente los eventos CloudTrail de un Security Hub. En EventBridge, puede crear reglas que respondan a los eventos registrados por CloudTrail.

AWS KMS entre los eventos se incluyen los siguientes:

- El material clave de una clave KMS se rotaba automáticamente
- El material clave importado en una clave de KMS ha caducado
- Se eliminó una clave de KMS cuya eliminación estaba programada

Estos eventos pueden iniciar acciones adicionales en su Cuenta de AWS. Estas acciones son diferentes de las CloudWatch alarmas descritas en la sección anterior porque solo se pueden activar después de que se produzca el evento. Por ejemplo, es posible que desee eliminar los recursos que están conectados a una clave específica después de que se haya eliminado esa clave, o puede que desee informar a un equipo de cumplimiento o auditoría de que la clave se ha eliminado.

También puede filtrar cualquier otro evento de la API en el que se haya iniciado sesión CloudTrail mediante EventBridge. Esto significa que si las acciones clave de la API relacionadas con las

políticas son motivo de preocupación específica, puedes filtrarlas. Por ejemplo, puedes filtrar la acción de EventBridge la `PutKeyPolicy` API. En términos más generales, puedes filtrar cualquier acción de la API que comience con `Disable*` o `Delete*` inicie respuestas automatizadas.

Con EventBridge ella, puede monitorizar (que es un control de detección) e investigar y responder (que son controles de respuesta) ante eventos inesperados o seleccionados. Por ejemplo, puede alertar a los equipos de seguridad y tomar medidas específicas si se crea un usuario o un rol de IAM, cuando se crea una clave de KMS o cuando se cambia una política clave. Puedes crear una regla de EventBridge eventos que filtre las acciones de la API que especifiques y, a continuación, asociar los objetivos a la regla. Los objetivos de ejemplo incluyen AWS Lambda funciones, notificaciones del Amazon Simple Notification Service (Amazon SNS), colas de Amazon Simple Queue Service (Amazon SQS) y más. Para obtener más información sobre el envío de eventos a los objetivos, consulta los destinos de Event Bus en Amazon EventBridge.

Para obtener más información sobre la supervisión AWS KMS EventBridge y la automatización de las respuestas, consulte Supervisar las claves de KMS con Amazon EventBridge en la AWS KMS documentación.

Mejores prácticas de administración de costos y facturación para AWS KMS

Gracias a su amplitud y profundidad, Servicios de AWS ofrezca la flexibilidad necesaria para gestionar sus costes y, al mismo tiempo, cumplir con los requisitos empresariales. En esta sección se describen los precios del almacenamiento de claves en AWS Key Management Service (AWS KMS) y se ofrecen recomendaciones para reducir los costes, por ejemplo, mediante el almacenamiento en caché de claves. También puedes revisar el uso de las claves de KMS para determinar si existen oportunidades adicionales para reducir los costos.

En esta sección se analizan los siguientes temas de administración de costos y facturación:

- AWS KMS precios del almacenamiento de claves
- Claves de bucket de Amazon S3 con cifrado predeterminado
- Almacenar en caché las claves de datos mediante AWS Encryption SDK
- Alternativas al almacenamiento en caché de claves y a las claves de bucket de Amazon S3
- Administrar los costos de registro para el uso de claves de KMS

AWS KMS precios del almacenamiento de claves

Cada uno de los AWS KMS key que cree AWS KMS tiene un coste. El cargo mensual es el mismo para las claves simétricas, las claves asimétricas, las claves HMAC, las claves multirregionales (cada clave principal y cada réplica de una clave multirregional), las claves con material de clave importado y las claves KMS con un origen de clave de un almacén de claves externo o AWS CloudHSM de uno externo.

En el caso de las claves KMS que se rotan automáticamente o a pedido, la primera y la segunda rotación de la clave añaden un coste mensual adicional (prorrateado por hora). Tras la segunda rotación, no se facturarán las rotaciones posteriores de ese mes. Consulte los AWS KMS precios para obtener la información más reciente sobre precios.

Se puede utilizar AWS Budgetspara configurar un presupuesto de uso. AWS Budgets puede avisarte cuando el gasto de tu cuenta supere determinados umbrales. En cuanto a los costes correspondientes AWS KMS, puedes crear un presupuesto de uso para enviar alertas en función de las claves o solicitudes del KMS. Esto puede mejorar la visibilidad de los costes de almacenamiento y uso de las AWS KMS claves.

Claves de bucket de Amazon S3 con cifrado predeterminado

En algunos casos de uso, las cargas de trabajo que acceden o generan un gran número de objetos en Amazon Simple Storage Service (Amazon S3) pueden generar grandes volúmenes de solicitudes, lo que AWS KMS aumenta los costes. La configuración de las claves de bucket de Amazon S3 puede ayudarle a reducir los costes hasta en un 99%. Esta es una alternativa recomendada a la desactivación del cifrado para ayudar a reducir los costes asociados AWS KMS a él.

Almacenar en caché las claves de datos mediante AWS Encryption SDK

Cuando se utiliza AWS Encryption SDKpara realizar el cifrado del lado del cliente, el almacenamiento en caché de las claves de datos puede ayudar a mejorar el rendimiento de la aplicación, reducir el riesgo de que las solicitudes de la aplicación AWS KMS se vean limitadas y ayudarle a reducir los costes. Para obtener más información sobre cómo empezar, consulte Cómo utilizar el almacenamiento en caché de claves de datos.

Alternativas al almacenamiento en caché de claves y a las claves de bucket de Amazon S3

Si el almacenamiento en caché de claves no es una opción para usted debido a sus requisitos de manejo de datos, también puede solicitar aumentos de AWS KMS cuota mediante la API Service Quotas AWS Management Console o la API Service Quotas. Ten en cuenta el volumen de llamadas a la API que podrías realizar. La cantidad de llamadas a la API que realices es un factor importante a la hora de AWS KMS fijar los precios. Si aumentas la cuota de solicitudes para aumentar tu rendimiento, el aumento del número de solicitudes generará costes AWS KMS adicionales.

Administrar los costos de registro para el uso de claves de KMS

Todas las llamadas a la AWS KMS API se registran en AWS CloudTrail. Las aplicaciones y los servicios pueden generar grandes volúmenes de llamadas a la AWS KMS API (por ejemplo, para operaciones criptográficas, incluidas las de cifrado y descifrado). Revisar los CloudTrail registros sin una herramienta que te ayude a organizar esos datos, investigar las tendencias y buscar actividad anómala en las API puede resultar difícil. Amazon Athena proporciona estructuras de datos predefinidas que pueden ayudarle a configurar rápidamente tablas para CloudTrail registros y

empezar a analizar sus datos de registro. Resulta especialmente útil para realizar análisis puntuales o realizar investigaciones adicionales durante la respuesta a un incidente. Para obtener más información, consulte AWS CloudTrail los registros de consultas en la documentación de Athena.

Como pagas por consulta por Athena, puedes configurar tus mesas por adelantado sin coste alguno. No se cobran cargos por las declaraciones en el lenguaje de definición de datos. Cuando responde a un incidente, esto le ayuda a asegurarse de que ya se cumplen muchos requisitos previos. Para ayudarle a prepararse, se recomienda escribir las consultas después de crear la tabla, probarlas y asegurarse de que producen los resultados que desea. Puede guardar sus consultas en Athena para usarlas en el futuro. Para obtener más información sobre cómo empezar a utilizar Athena, consulte Introducción a Amazon Athena.

Los eventos de datos proporcionan visibilidad de las operaciones que se realizan en un recurso o dentro de él. Se denominan también operaciones del plano de datos. Algunos ejemplos son los `PutObject` eventos de Amazon S3 o las llamadas a la API de operaciones de funciones de Lambda. Los eventos de datos suelen ser actividades de gran volumen y se le cobrará por registrarlos. Para ayudar a controlar el volumen de eventos de datos que se registran en las rutas o en los almacenes de datos de eventos CloudTrail, puede optimizar el registro para CloudTrail reducir los costes y configurar Amazon S3 mediante la configuración de selectores de eventos avanzados para limitar los eventos de datos en CloudTrail los que iniciar sesión. AWS KMS Para obtener más información, consulte Cómo optimizar AWS CloudTrail los costes mediante el uso de selectores de eventos avanzados (entrada del AWS blog).

Recursos

AWS Key Management Service (AWS KMS) documentación

- AWS KMS Guía para desarrolladores
- Referencia de la API de AWS KMS
- AWS KMS en la AWS CLI Referencia

Herramientas

- AWS Encryption SDK

AWS Guía prescriptiva

Estrategias

- Crear una estrategia de cifrado para los datos en reposo

Guías

- Características y prácticas recomendadas de cifrado para Servicios de AWS
- AWS Arquitectura de referencia de privacidad (AWS PRA)

Patrones

- Cifre automáticamente los volúmenes de Amazon EBS
- Automatically remediate unencrypted Amazon RDS DB instances and clusters
- Supervise y corrija la eliminación programada de AWS KMS keys

Colaboradores

Creación

- Frank Phillis, arquitecto sénior de soluciones especializado en GTM, AWS
- Ken Beer, director de bibliotecas AWS KMS criptográficas, AWS
- Michael Miller, arquitecto sénior de soluciones, AWS
- Jeremy Stieglitz, director principal de productos, AWS
- Zach Miller, arquitecto principal de soluciones, AWS
- Peter M. O'Donnell, arquitecto principal de soluciones, AWS
- Patrick Palmer, arquitecto principal de soluciones, AWS
- Dave Walker, arquitecto principal de soluciones, AWS

Revisando

- Manigandan Shri, consultora sénior de entregas, AWS

Redacción técnica

- Lilly AbouHarb, redactora técnica sénior, AWS
- Kimberly Garmoe, redactora técnica sénior, AWS

Historial de documentos

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

Cambio	Descripción	Fecha
Publicación inicial	—	24 de marzo de 2025

AWS Glosario de orientación prescriptiva

Los siguientes son términos de uso común en las estrategias, guías y patrones proporcionados por la Guía AWS prescriptiva. 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 PostgreSQL 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 (Amazon RDS) para Oracle en el. Nube de AWS
- Recomprar (readquirir): cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: migre su sistema de gestión de relaciones con los clientes (CRM) a Salesforce.com.
- Volver a alojar (migrar mediante lift-and-shift): traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Oracle en una EC2 instancia del. Nube de AWS
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma local a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

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

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

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

migración activa-pasiva

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

función de agregación

Función SQL 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 ABAC AWS en la documentación 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 a 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 CAF organiza 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 preparar a la organización para una adopción exitosa de la nube. Para obtener más información, consulte la Página web de AWS CAF y el Documento técnico de AWS CAF.

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 WQF se 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 llamadas sospechosas a la API 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 endianness.

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.

branch

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.

captura de datos de cambio (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. Puede utilizar los CDC para diversos 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 publicaciones de CCo E en el 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 una CCo E, establecer un 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 oBitbucket 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, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

desviación de configuración

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

base de datos de administración de configuración (CMDB)

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, los

datos de una CMDB se utilizan en la etapa de detección y análisis de la cartera de productos durante la migración.

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 región Cuenta de AWS y, o en una organización, mediante una plantilla YAML. Para obtener más información, consulta los paquetes de conformidad en la documentación. AWS Config

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD se describe comúnmente como una canalización. CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar más rápido. 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 una administración y un gobierno centralizados.

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de datos (DDL)

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

lenguaje de manipulación 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.

asignación de flujos de valor para el 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. DVSM amplía el proceso de asignación 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 Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) 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.

EDI

Véase intercambio electrónico 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.

intercambio electrónico de datos (EDI)

El intercambio automatizado de documentos comerciales entre organizaciones. Para obtener más información, consulte Qué es el intercambio electrónico de datos.

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

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

planificación de recursos empresariales (ERP)

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

cifrado de sobre

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

entorno

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 un CI/CD proceso, 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 epopeyas AWS de seguridad de CAF 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.

PERP

Consulte planificación de recursos empresariales.

análisis de datos de tipo exploratorio (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. El EDA se 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, esto 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.

indicaciones de unos pocos pasos

Proporcionar a un LLM un pequeño número de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que realice una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, en el que los modelos aprenden a partir de ejemplos (planos) integrados en las instrucciones. Las indicaciones con pocas tomas pueden ser eficaces para tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también el apartado de mensajes sin intervención.

FGAC

Consulte el control de acceso detallado.

control de acceso preciso (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.

FM

Consulte el modelo básico.

modelo de base (FM)

Una gran red neuronal de aprendizaje profundo que se ha estado entrenando con conjuntos de datos masivos de datos generalizados y sin etiquetar. FMs son capaces de realizar una amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural. Para obtener más información, consulte Qué son los modelos básicos.

G

IA generativa

Un subconjunto de modelos de IA que se han entrenado con grandes cantidades de datos y que pueden utilizar un simple mensaje de texto para crear contenido y artefactos nuevos, como imágenes, vídeos, texto y audio. Para obtener más información, consulte Qué es la IA generativa.

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.

imagen dorada

Instantánea de un sistema o software que se utiliza como plantilla para implementar nuevas instancias de ese sistema o software. Por ejemplo, en la fabricación, una imagen dorada se puede utilizar para aprovisionar software en varios dispositivos y ayuda a mejorar la velocidad, la escalabilidad y la productividad de las operaciones de fabricación de dispositivos.

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 permisos de IAM. 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

HA

Consulte la 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.

datos retenidos

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de aprendizaje automático. Puede utilizar los datos de reserva para evaluar el rendimiento del modelo comparando las predicciones del modelo con los datos de reserva.

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 para 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, las revisiones se suelen realizar fuera del flujo de trabajo habitual de las versiones. DevOps

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 identidades

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

aplicación inactiva

Aplicación que utiliza un promedio de CPU y memoria de entre 5 y 20 por ciento durante un periodo 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 .

VPC entrante (de entrada)

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 y el resto de Internet.

migración gradual

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

Industria 4.0

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

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial (T) IIo

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 de la Internet de las cosas (IIoT) industrial.

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red VPCs entre Internet y las redes locales (en una misma o Regiones de AWS diferente). La arquitectura AWS de referencia de seguridad recomienda configurar su 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. La ITIL proporciona la base para la ITSM.

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 las herramientas de ITSM, 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.

modelo de lenguaje grande (LLM)

Un modelo de IA de aprendizaje profundo que se entrena previamente con una gran cantidad de datos. Un LLM puede realizar múltiples tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para obtener más información, consulte Qué son. LLMs

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 de privilegio mínimo en la documentación de IAM.

migrar mediante lift-and-shift

Ver 7 Rs.

sistema little-endian

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

LLM

Véase un modelo de lenguaje amplio.

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 registradores de pulsaciones de teclas.

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 los ajustes necesarios. 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 telemétrico de Message Queue Queue (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

Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. El MAP incluye 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 más comunes.

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 incluir a analistas y propietarios de operaciones, empresas, 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.

Migration Portfolio Assessment (MPA)

Una herramienta en línea que proporciona información para validar el modelo de negocio para migrar a. Nube de AWS La MPA ofrece una evaluación detallada de la cartera (adecuación del

tamaño de los servidores, precios, comparaciones del costo total de propiedad, 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 oleadas). La herramienta MPA (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores asociados de APN.

Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar sus puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas mediante el AWS CAF. Para obtener más información, consulte la Guía de preparación para la migración. La MRA es la primera fase de la estrategia de migración de AWS.

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.

MAPA

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

Véase 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. El OPC-UA proporciona un estándar de interoperabilidad con esquemas de cifrado, autenticación y autorización de datos.

acuerdo de nivel operativo (OLA)

Acuerdo que aclara lo que los grupos de TI operativos se comprometen a ofrecerse 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.

administración del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. La OCM ayuda a las empresas a prepararse para nuevos sistemas y estrategias y a realizar la transición a ellos, al acelerar la adopción de cambios, abordar los problemas de transición e impulsar cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración de personal, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la Guía de OCM.

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). El OAC admite todos los buckets de S3 Regiones de AWS, el cifrado del lado del servidor AWS KMS (SSE-KMS) y las solicitudes dinámicas `PUT` y `DELETE` dirigidas al bucket de S3.

identidad de acceso de origen (OAI)

En CloudFront, una opción para restringir el acceso y proteger el contenido de Amazon S3. Cuando utiliza OAI, 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 el OAC, que proporciona un control de acceso más detallado y mejorado.

ORR

Consulte la revisión de la preparación operativa.

OT

Consulte la tecnología operativa.

VPC saliente (de salida)

En una arquitectura de AWS cuentas múltiples, una VPC que gestiona las conexiones de red que se inician desde 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.

P

límite de permisos

Una política de administración de IAM que se adjunta a las entidades principales de IAM para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte Límites de permisos en la documentación de IAM.

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 de información de identificación personal son los nombres, las direcciones y la 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.

policy

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 para un Cuenta de AWS rol de IAM o un usuario. Para obtener más información, consulte Entidad principal en Términos y conceptos de roles en la documentación de IAM.

privacidad desde el diseño

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

zonas alojadas privadas

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a las consultas de DNS de un dominio y sus subdominios dentro de uno o más VPCs. 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 que no cumplan con las normas. 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 fabricación, una computadora adaptable y altamente confiable que monitorea las máquinas y automatiza los procesos de fabricación.

encadenamiento rápido

Utilizar la salida de un mensaje de LLM como entrada para el siguiente mensaje para generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en subtareas o para

refinar o ampliar de forma iterativa una respuesta preliminar. Ayuda a mejorar la precisión y la relevancia de las respuestas de un modelo y permite obtener resultados más detallados y personalizados.

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 MES basado en microservicios, 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 relacional SQL.

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

Matriz RACI

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

RAG

Consulte Retrieval Augmented Generation.

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.

Matriz RASCI

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

RCAC

Consulte control de acceso por filas y columnas.

réplica de lectura

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 y es 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.

resiliencia

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, confiable, consultada e 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 matriz RASCI y, si la excluye, se denomina matriz RACI.

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.

Generación aumentada de recuperación (RAG)

Tecnología de inteligencia artificial generativa en la que un máster hace referencia a una fuente de datos autorizada que se encuentra fuera de sus fuentes de datos de formación antes de generar una respuesta. Por ejemplo, un modelo RAG podría realizar una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para obtener más información, consulte Qué es el RAG.

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 expresiones SQL básicas y flexibles que tienen reglas de acceso definidas. El RCAC consta 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

SAML 2.0

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 operaciones de la AWS API sin tener que crear un usuario en IAM para todos los miembros de la organización. Para obtener más información sobre la federación basada en SAML 2.0, consulte Acerca de la federación basada en SAML 2.0 en la documentación de 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.

seguridad desde el diseño

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

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. Existen cuatro tipos principales de controles de seguridad: preventivos, de detección, con capacidad 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 sobre seguridad y administración de eventos (SIEM)

Herramientas y servicios que combinan sistemas de administración de información sobre seguridad (SIM) y de administración de eventos de seguridad (SEM). Un sistema de SIEM

recopila, monitorea y analiza los datos de servidores, redes, dispositivos y otras fuentes para detectar amenazas y brechas de seguridad y generar alertas.

automatización de la respuesta 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 automatizadas incluyen la modificación de un grupo de seguridad de VPC, 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 quien Servicio de AWS los recibe.

política de control de servicio (SCP)

Política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPs defina 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

La 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 falla.

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 con la aplicación de este patrón, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

subred

Un intervalo de direcciones IP en la VPC. Una subred debe residir en una sola zona de disponibilidad.

supervisión, control 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.

indicador del sistema

Una técnica para proporcionar contexto, instrucciones o pautas a un LLM para dirigir su comportamiento. Las indicaciones del sistema ayudan a establecer el contexto y las reglas para las interacciones con los usuarios.

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.

Interconexión con VPC

Una conexión entre dos VPCs que le permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulte ¿Qué es una interconexión de VPC? en la documentación de Amazon VPC.

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

Función SQL 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.

GUSANO

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.

aviso de tiro cero

Proporcionar a un LLM instrucciones para realizar una tarea, pero sin ejemplos (imágenes) que puedan ayudar a guiarla. El LLM debe utilizar sus conocimientos previamente entrenados para

realizar la tarea. La eficacia de las indicaciones cero depende de la complejidad de la tarea y de la calidad de las indicaciones. Consulte también las indicaciones de pocos pasos.

aplicación zombi

Aplicación que utiliza un promedio de CPU y memoria menor 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.