Controles de seguridad recomendados para implementar las capacidades de seguridad de la AWS CAF

AWS Guía prescriptiva

AWS Guía prescriptiva: Controles de seguridad recomendados para implementar las capacidades de seguridad de la AWS CAF

Table of Contents

Controles de seguridad recomendados para implementar las capacidades de seguridad AWS de CAF

Rishi Singla y Rovan Omar, Amazon Web Services ()AWS

Noviembre de 2023 (historial de documentos)

La seguridad es la máxima prioridad en. AWS Para ayudar a aliviar su carga operativa, usted comparte la responsabilidad de la seguridad y el cumplimiento de la nube AWS. AWS es responsable de la seguridad de la nube, lo que significa proteger la infraestructura en la que se ejecutan los servicios que se ofrecen en la nube Nube de AWS. Usted es responsable de la seguridad en la nube, por ejemplo, de sus datos y aplicaciones. Esta guía proporciona controles de seguridad que pueden ayudarlo a cumplir con sus responsabilidades de seguridad en la Nube de AWS.

El marco de adopción de la AWS nube (AWS CAF) proporciona las mejores prácticas diseñadas para mejorar su preparación para la nube. AWS CAF clasifica esas mejores prácticas en seis perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Esta guía se centra en las siguientes capacidades desde la perspectiva de la seguridad:

- Gestión de identidades y accesos: gestione las identidades humanas y de máquinas y sus permisos a escala.
- Detección de amenazas: configure el registro y la supervisión para detectar e investigar un posible error de configuración de seguridad, una amenaza o un comportamiento inesperado.
- Protección de la infraestructura: proteja los sistemas y servicios del acceso no deseado o no autorizado y de las posibles vulnerabilidades.
- Protección de datos: clasifique los datos en función de los niveles de confidencialidad. Mantenga la visibilidad y el control de los datos y de cómo se accede a ellos y se utilizan en su organización.
- Respuesta a incidentes: establezca mecanismos para responder y mitigar el impacto potencial de los incidentes de seguridad.

Si no se implementan controles de seguridad preventivos, de detección y con capacidad de respuesta para estas capacidades de seguridad de la AWS CAF, puede suponer un riesgo crítico para su entorno de nube y provocar interrupciones en su negocio. La implementación de los controles de seguridad de esta guía puede ayudar a su organización a proteger su entorno de nube.

> **Note**
>
> AWS proporciona servicios, herramientas y marcos que pueden ayudarlo a operar de forma segura en el Nube de AWS. Esta guía se alinea con el Marco de Buena AWS Arquitectura AWS , el Marco de Adopción de la Nube AWS (CAF), AWS la Arquitectura de Referencia de Seguridad AWS (SRA) y otras recomendaciones de seguridad publicadas por. AWS Los controles de esta guía no incluyen todas las consideraciones de seguridad en la nube y no pretende reemplazar estos marcos.

Recomendaciones de control de seguridad para gestionar la identidad y el acceso

Puede crear identidades en AWS una fuente de identidad externa o conectarse a ella. Mediante las políticas AWS Identity and Access Management (de IAM), se conceden a los usuarios los permisos necesarios para que puedan acceder a AWS los recursos y las aplicaciones integradas o gestionarlos. Una gestión eficaz de la identidad y el acceso ayuda a validar que las personas y las máquinas adecuadas tengan acceso a los recursos adecuados en las condiciones adecuadas. El AWS Well-Architected Framework proporciona las mejores prácticas para administrar las identidades y sus permisos. Los ejemplos de mejores prácticas incluyen confiar en un proveedor de identidad centralizado y utilizar mecanismos de inicio de sesión sólidos, como la autenticación multifactor (MFA). Los controles de seguridad de esta sección pueden ayudarte a implementar estas prácticas recomendadas.

Controles de esta sección:

- Supervise y configure las notificaciones de la actividad del usuario root
- No crear claves de acceso para el usuario raíz
- Habilitar MFA para el usuario root
- Siga las prácticas recomendadas de seguridad para IAM
- Otorgue permisos con privilegios mínimos
- Defina las barreras de protección de permisos a nivel de carga de trabajo
- Cambie las claves de acceso de IAM a intervalos regulares
- Identifique los recursos que se comparten con una entidad externa

Supervise y configure las notificaciones de la actividad del usuario root

Al crear una por primera vez Cuenta de AWS, se comienza con una identidad de inicio de sesión única denominada usuario raíz. De forma predeterminada, el usuario raíz tiene acceso total a todos Servicios de AWS los recursos de la cuenta. Debe controlar y supervisar rigurosamente al usuario raíz y usarlo solo para tareas que requieran credenciales de usuario raíz.

Para obtener más información, consulte los siguientes recursos:

- Otorgue el acceso con menos privilegios en el Well-Architected Framework AWS
- Supervise la actividad de los usuarios raíz de IAM en Prescriptive Guidance AWS

No crear claves de acceso para el usuario raíz

El usuario raíz es el usuario de Cuenta de AWS con más privilegios. La desactivación del acceso programático al usuario raíz ayuda a reducir el riesgo de que las credenciales del usuario queden expuestas de forma inadvertida y, posteriormente, de que se ponga en peligro el entorno de nube. Le recomendamos que cree y utilice funciones de IAM como credenciales temporales para acceder a sus recursos y a ellos. Cuentas de AWS

Para obtener más información, consulte los siguientes recursos:

- La clave de acceso del usuario raíz de IAM no debería figurar en la documentación AWS Security Hub
- Eliminar las claves de acceso del usuario raíz en la documentación de IAM
- Funciones de IAM en la documentación de IAM

Habilitar MFA para el usuario root

Le recomendamos que habilite varios dispositivos de autenticación multifactor (MFA) para Cuenta de AWS el usuario raíz y los usuarios de IAM. Esto eleva el nivel de seguridad Cuentas de AWS y puede simplificar la administración del acceso. Dado que un usuario root es un usuario con muchos privilegios que puede realizar acciones privilegiadas, es crucial requerir MFA para el usuario root. Puede usar un dispositivo MFA de hardware que genere un código numérico basado en el algoritmo de contraseña de un solo uso (TOTP) basada en el tiempo, una clave de seguridad de hardware FIDO o una aplicación de autenticación virtual.

En 2024, se requerirá la MFA para acceder al usuario raíz de cualquier usuario. Cuenta de AWS Para obtener más información, consulte Secure by Design: AWS para mejorar los requisitos de MFA en 2024 en el blog de AWS seguridad. Le recomendamos encarecidamente que amplíe esta práctica de seguridad y exija la MFA para todos los tipos de usuarios de sus AWS entornos.

Si es posible, le recomendamos que utilice un dispositivo MFA de hardware para el usuario root. Una aplicación de MFA virtual podría no proporcionar el mismo nivel de seguridad que un dispositivo

MFA físico. Puede utilizar el MFA virtual mientras espera la aprobación o la entrega de la compra del hardware.

En situaciones en las que administras cientos de cuentas AWS Organizations, según la tolerancia al riesgo de tu organización, es posible que no sea escalable usar MFA basada en hardware para el usuario raíz de cada cuenta de una unidad organizativa (OU). En este caso, puede elegir una cuenta de la OU que actúe como cuenta de administración de la OU y, a continuación, deshabilitar al usuario raíz para las demás cuentas de esa OU. De forma predeterminada, la cuenta de administración de la unidad organizativa no tiene acceso a las demás cuentas. Si configura el acceso multicuenta por adelantado, podrá acceder a las demás cuentas desde la cuenta de administración de la OU en caso de emergencia. Para configurar el acceso entre cuentas, debe crear un rol de IAM en la cuenta del miembro y definir políticas para que solo el usuario raíz de la cuenta de administración de la OU pueda asumir este rol. Para obtener más información, consulte el tutorial: Delegar el acceso Cuentas de AWS mediante el uso de funciones de IAM en la documentación de IAM.

Le recomendamos que habilite varios dispositivos MFA para sus credenciales de usuario raíz. Puede registrar hasta ocho dispositivos MFA de cualquier combinación.

Para obtener más información, consulte los siguientes recursos:

- Habilitar un token TOTP de hardware en la documentación de IAM
- Habilitación de un dispositivo virtual de autenticación multifactor (MFA) en la documentación de IAM
- Habilitar una clave de seguridad FIDO en la documentación de IAM
- Proteja el inicio de sesión del usuario raíz con la autenticación multifactor (MFA) en la documentación de IAM

Siga las prácticas recomendadas de seguridad para IAM

La documentación de IAM incluye una lista de las mejores prácticas diseñadas para ayudarle a proteger sus recursos Cuentas de AWS . Incluye recomendaciones para configurar el acceso y los permisos de acuerdo con el principio del privilegio mínimo. Algunos ejemplos de prácticas recomendadas de seguridad de IAM incluyen la configuración de la federación de identidades, la exigencia de MFA y el uso de credenciales temporales.

Para obtener más información, consulte los siguientes recursos:

- Las mejores prácticas de seguridad en IAM en la documentación de IAM

- Uso de credenciales temporales con AWS los recursos de la documentación de IAM

Otorgue permisos con privilegios mínimos

El privilegio mínimo es la práctica de conceder solo los permisos necesarios para realizar una tarea. Para ello, defina las acciones que se pueden realizar en recursos específicos en condiciones específicas.

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define los permisos en función de los atributos, como sus etiquetas. Puede utilizar los atributos de grupo, identidad y recursos para definir dinámicamente los permisos a escala, en lugar de definir permisos para usuarios individuales. Por ejemplo, puedes usar ABAC para permitir que un grupo de desarrolladores acceda solo a los recursos que tengan una etiqueta específica asociada a su proyecto.

Para obtener más información, consulte los siguientes recursos:

- Aplica los permisos con privilegios mínimos en la documentación de IAM
- ¿Para qué sirve ABAC en la documentación de IAM AWS

Defina las barreras de protección de permisos a nivel de carga de trabajo

La mejor práctica es utilizar una estrategia de cuentas múltiples, ya que proporciona flexibilidad para definir barreras a nivel de carga de trabajo. La arquitectura AWS de referencia de seguridad ofrece una guía prescriptiva sobre cómo estructurar las cuentas. Estas cuentas se administran como una organización y AWS Organizationsse agrupan en unidades organizativas (OUs).

Servicios de AWS, por ejemplo AWS Control Tower, pueden ayudarte a gestionar de forma centralizada los controles de una organización. Le recomendamos que defina un propósito claro para cada cuenta o unidad organizativa de la organización y que aplique los controles de acuerdo con ese propósito. AWS Control Tower implementa controles preventivos, de detección y proactivos que le ayudan a controlar los recursos y a supervisar el cumplimiento. Un control preventivo está diseñado para evitar que se produzca un evento. Un control de detección está diseñado para detectar, registrar y alertar después de que se haya producido un evento. Un control proactivo está diseñado para

evitar el despliegue de recursos no conformes mediante el análisis de los recursos antes de su aprovisionamiento.

Para obtener más información, consulte los siguientes recursos:

- Separe las cargas de trabajo mediante cuentas del AWS Well-Architected Framework
- AWS La arquitectura de referencia de seguridad (AWS SRA) en una guía prescriptiva AWS
- Acerca de los controles AWS Control Tower en la documentación AWS Control Tower
- La implementación de los controles de seguridad figura AWS en la AWS Guía prescriptiva
- Utilice las políticas de control de servicios para establecer barreras de protección de permisos en todas las cuentas de su AWS organización en el blog de seguridad AWS

Cambie las claves de acceso de IAM a intervalos regulares

Se recomienda actualizar las claves de acceso para los casos de uso que requieren credenciales a largo plazo. Recomendamos rotar las claves de acceso cada 90 días o menos. La rotación de las claves de acceso reduce el riesgo de que se utilice una clave de acceso asociada a una cuenta comprometida o cancelada. También impide el acceso mediante el uso de una clave antigua que podría haberse perdido, estar en peligro o haber sido robada. Actualice siempre las aplicaciones después de girar las claves de acceso.

Para obtener más información, consulte los siguientes recursos:

- Actualice las claves de acceso cuando sea necesario para los casos de uso que requieran credenciales a largo plazo en la documentación de IAM
- Gire automáticamente las claves de acceso de los usuarios de IAM a escala con AWS Organizations y según la Guía AWS Secrets Manager prescriptiva AWS
- Actualización de las claves de acceso en la documentación de IAM

Identifique los recursos que se comparten con una entidad externa

Una entidad externa es un recurso, una aplicación, un servicio o un usuario que se encuentra fuera de AWS la organización, por ejemplo Cuentas de AWS, un usuario raíz, un usuario o rol de IAM, un usuario federado o un Servicio de AWS usuario anónimo (o no autenticado). Es una práctica recomendada de seguridad utilizar IAM Access Analyzer para identificar los recursos de la

organización y las cuentas, como los depósitos de Amazon Simple Storage Service (Amazon S3) o las funciones de IAM, que se comparten con una entidad externa. Esto le ayuda a identificar el acceso no deseado a los recursos y los datos, lo que constituye un riesgo para la seguridad.

Para obtener más información, consulte los siguientes recursos:

- Verifique el acceso público y entre cuentas a los recursos con IAM Access Analyzer en la documentación de IAM
- Analice el acceso público y multicuenta en el AWS Well-Architected Framework
- Utilizándolo AWS Identity and Access Management Access Analyzer en la documentación de IAM

Recomendaciones de control de seguridad para el registro y la supervisión

El registro y la supervisión son aspectos importantes de la detección de amenazas. La detección de amenazas es una de las capacidades desde el punto de vista de la seguridad del AWS Cloud Adoption Framework (AWS CAF). Al usar datos de registro, su organización puede monitorear su entorno para comprender e identificar posibles errores de configuración de seguridad, amenazas y comportamientos inesperados. Comprender las posibles amenazas puede ayudar a su organización a priorizar los controles de seguridad, y una detección eficaz de las amenazas puede ayudarle a responder a las amenazas con mayor rapidez.

Controles de esta sección:

- Configure al menos una ruta multirregional en CloudTrail
- Configure el registro a nivel de servicio y aplicación
- Establezca una ubicación centralizada para analizar los registros y responder a los eventos de seguridad
- Impida el acceso no autorizado a los depósitos de S3 que contienen archivos de CloudTrail registro
- Configure alertas para los cambios en los grupos de seguridad o la red ACLs
- Configure alertas para CloudWatch las alarmas que entran en el estado de ALARMA

Configure al menos una ruta multirregional en CloudTrail

AWS CloudTraille ayuda a auditar la gobernanza, el cumplimiento y el riesgo operativo de su Cuenta de AWS empresa. Las acciones realizadas por un usuario, un rol o una Servicio de AWS persona se registran como eventos en CloudTrail. Los eventos incluyen las acciones realizadas en AWS Management Console, AWS Command Line Interface (AWS CLI) y AWS SDKs y APIs. Este historial de eventos le ayuda a analizar su postura de seguridad, realizar un seguimiento de los cambios en los recursos y auditar el cumplimiento.

Para tener un registro continuo de los eventos que se produzcan en su entorno Cuenta de AWS, debe crear un registro. Cada ruta debe configurarse para registrar todos los eventos Regiones de AWS. Al registrar todos los eventos Regiones de AWS, se asegura de que se registren todos los eventos que se produzcan en su Cuenta de AWS interior, independientemente del lugar en el que se

Región de AWS hayan producido. Un registro multirregional garantiza que se registren los eventos del servicio global.

Para obtener más información, consulte los siguientes recursos:

- CloudTrail las mejores prácticas de seguridad policial en la documentación CloudTrail
- Convertir una ruta que se aplica a una región para que se aplique a todas las regiones de la CloudTrail documentación
- Habilitar y deshabilitar el registro de eventos del servicio global en la documentación CloudTrail

Configure el registro a nivel de servicio y aplicación

El AWS Well-Architected Framework recomienda conservar los registros de eventos de seguridad de los servicios y las aplicaciones. Este es un principio fundamental de seguridad para las auditorías, las investigaciones y los casos de uso operativo. La retención de los registros de servicios y aplicaciones es un requisito de seguridad común que se basa en los estándares, políticas y procedimientos de gobernanza, riesgo y cumplimiento (GRC).

Los equipos de operaciones de seguridad utilizan los registros y las herramientas de búsqueda para descubrir posibles eventos de interés que puedan indicar una actividad no autorizada o un cambio involuntario. Puede habilitar el registro para distintos servicios, según el caso de uso. Por ejemplo, puede registrar el acceso al bucket de Amazon S3, el tráfico de ACL AWS WAF web, el tráfico de Amazon API Gateway en la capa de red o CloudFront las distribuciones de Amazon.

Para obtener más información, consulte los siguientes recursos:

- Transmita Amazon CloudWatch Logs a una cuenta centralizada para realizar auditorías y análisis en el blog de AWS arquitectura
- Configurar el registro de servicios y aplicaciones en AWS Well-Architected Framework

Establezca una ubicación centralizada para analizar los registros y responder a los eventos de seguridad

El análisis manual de los registros y el procesamiento de la información no son suficientes para mantener el volumen de información asociado a las arquitecturas complejas. El análisis y la elaboración de informes por sí solos no facilitan la asignación de eventos al recurso correcto de

manera oportuna. El AWS Well-Architected Framework recomienda AWS integrar los eventos y hallazgos de seguridad en un sistema de notificación y flujo de trabajo, como un sistema de gestión de eventos e información de seguridad (SIEM), errores o sistemas de gestión de eventos e información de seguridad (SIEM). Estos sistemas le ayudan a asignar, enrutar y gestionar los eventos de seguridad.

Para obtener más información, consulte los siguientes recursos:

- Analice los registros, los hallazgos y las métricas de forma centralizada en AWS Well-Architected Framework
- Analice la seguridad, el cumplimiento y la actividad operativa con CloudTrail Amazon Athena en el AWS blog de seguridad
- AWS Socios que ofrecen servicios de detección y respuesta a amenazas en la cartera de AWS socios

Impida el acceso no autorizado a los depósitos de S3 que contienen archivos de CloudTrail registro

De forma predeterminada, los archivos de CloudTrail registro se almacenan en buckets de Amazon S3. Impedir el acceso no autorizado a cualquier bucket de Amazon S3 que contenga archivos de CloudTrail registro constituye una práctica recomendada de seguridad. Esto le ayuda a mantener la integridad, integridad y disponibilidad de estos registros, lo cual es crucial para fines forenses y de auditoría. Si desea registrar los eventos de datos de los depósitos de S3 que contienen archivos de CloudTrail registro, puede crear un registro CloudTrail para ello.

Para obtener más información, consulte los siguientes recursos:

- Configuración de los ajustes de acceso público en bloque para sus buckets de S3 en la documentación de Amazon S3
- CloudTrail las mejores prácticas de seguridad preventiva en la documentación CloudTrail
- Crear una pista en la documentación CloudTrail

Configure alertas para los cambios en los grupos de seguridad o la red ACLs

Un grupo de seguridad de Amazon Virtual Private Cloud (Amazon VPC) controla el tráfico que puede llegar y salir de los recursos a los que está asociado. Una lista de control de acceso a la red (ACL) permite o deniega tráfico entrante o saliente específico en el nivel de subred de la VPC. Estos recursos son fundamentales para administrar el acceso en su entorno. AWS

Cree y configure una CloudWatch alarma de Amazon que le notifique si la configuración de un grupo de seguridad o ACL de red cambia. Configure esta alarma para que le avise cada vez que se realice una llamada a la AWS API para actualizar los grupos de seguridad. También puede utilizar servicios, como Amazon EventBridge y AWS Config, para responder automáticamente a este tipo de eventos de seguridad.

Para obtener más información, consulte los siguientes recursos:

- Revierta automáticamente y reciba notificaciones sobre los cambios en sus grupos de seguridad de Amazon VPC en AWS el blog de seguridad
- Uso de CloudWatch las alarmas de Amazon en la CloudWatch documentación
- Implemente eventos de seguridad procesables en el AWS Well-Architected Framework
- Automatice la respuesta a los eventos en el AWS Well-Architected Framework

Configure alertas para CloudWatch las alarmas que entran en el estado de ALARMA

En CloudWatch, puede especificar qué acciones realiza una alarma cuando cambia de estado entre los `INSUFFICIENT_DATA` estados `OKALARM`, y. El tipo de acción de alarma más común consiste en notificar a una o más personas mediante el envío de un mensaje a un tema de Amazon Simple Notification Service (Amazon SNS). También puede configurar alarmas para que se generen OpsItemso generen AWS Systems Manager incidentes.

Le recomendamos que active las acciones de alarma para alertar automáticamente si una métrica monitorizada está fuera del umbral definido. La supervisión de las alarmas le ayuda a identificar actividades inusuales y a responder rápidamente a los problemas operativos y de seguridad.

Para obtener más información, consulte los siguientes recursos:

- Implemente eventos de seguridad procesables en el AWS Well-Architected Framework
- Acciones de alarma en la documentación CloudWatch

Recomendaciones de control de seguridad para proteger la infraestructura

La protección de la infraestructura es una parte clave de cualquier programa de seguridad. Incluye metodologías de control que le ayudan a proteger sus redes y recursos informáticos. Algunos ejemplos de protección de infraestructuras son los límites de confianza, un defense-in-depth enfoque, el refuerzo de la seguridad, la administración de parches y la autenticación y autorización del sistema operativo. Para obtener más información, consulte Protección de la infraestructura en el AWS Well-Architected Framework. Los controles de seguridad de esta sección pueden ayudarle a implementar las mejores prácticas para la protección de la infraestructura.

Controles de esta sección:

- Especifique los objetos raíz predeterminados para las CloudFront distribuciones
- Escanee el código de la aplicación para identificar problemas de seguridad comunes
- Cree capas de red mediante subredes y subredes dedicadas VPCs
- Restrinja el tráfico entrante solo a los puertos autorizados
- Bloquear el acceso público a los documentos de Systems Manager
- Bloquear el acceso público a las funciones de Lambda
- Restrinja el tráfico entrante y saliente en el grupo de seguridad predeterminado
- Escanee en busca de vulnerabilidades de software y de exposición no intencionada a la red
- Configure AWS WAF
- Configure protecciones avanzadas contra los ataques S DDo
- Utilice un defense-in-depth enfoque para controlar el tráfico de la red

Especifique los objetos raíz predeterminados para las CloudFront distribuciones

Amazon CloudFront acelera la distribución de tu contenido web al distribuirlo a través de una red mundial de centros de datos, lo que reduce la latencia y mejora el rendimiento. Si no define un objeto raíz predeterminado, las solicitudes de la raíz de su distribución pasarán a su servidor de origen. Si utilizas un origen de Amazon Simple Storage Service (Amazon S3), la solicitud podría devolver una

lista del contenido de tu bucket de S3 o una lista del contenido privado de tu origen. Especificar un objeto raíz predeterminado le ayuda a evitar que se exponga el contenido de su distribución.

Para obtener más información, consulte los siguientes recursos:

- Especificar un objeto raíz predeterminado en la CloudFront documentación

Escanee el código de la aplicación para identificar problemas de seguridad comunes

El AWS Well-Architected Framework recomienda escanear las bibliotecas y las dependencias en busca de problemas y defectos. Existen muchas herramientas de análisis de código fuente que puede utilizar para escanear el código fuente. Por ejemplo, Amazon CodeGuru puede buscar problemas de seguridad comunes en Java o Python aplicaciones y proporciona recomendaciones para su corrección.

Para obtener más información, consulte los siguientes recursos:

- CodeGuru documentación
- herramientas de análisis de código fuente en OWASP Foundation sitio web
- Realice la gestión de vulnerabilidades en el AWS Well-Architected Framework

Cree capas de red mediante subredes y subredes dedicadas VPCs

El AWS Well-Architected Framework recomienda agrupar los componentes que comparten requisitos de sensibilidad en capas. Esto minimiza el alcance potencial del impacto del acceso no autorizado. Por ejemplo, un clúster de base de datos que no requiere acceso a Internet debe colocarse en una subred privada de su VPC para garantizar que no haya una ruta hacia o desde Internet.

AWS ofrece muchos servicios que pueden ayudarle a probar e identificar la accesibilidad pública. Por ejemplo, Reachability Analyzer es una herramienta de análisis de configuración que le ayuda a probar la conectividad entre los recursos de origen y destino de su. VPCs Además, Network Access Analyzer puede ayudarlo a identificar el acceso no deseado a la red a los recursos.

Para obtener más información, consulte los siguientes recursos:

- Cree capas de red en AWS Well-Architected Framework

- Documentación del Reachability Analyzer
- Documentación sobre Network Access Analyzer
- Creación de una subred en la documentación de Amazon Virtual Private Cloud (Amazon VPC)

Restrinja el tráfico entrante solo a los puertos autorizados

El acceso sin restricciones, como el tráfico de la dirección IP de `0.0.0.0/0` origen, aumenta el riesgo de actividad maliciosa, como la piratería informática, los ataques denial-of-service (DoS) y la pérdida de datos. Los grupos de seguridad proporcionan un filtrado detallado del tráfico de la red que ingresa y sale a los recursos. AWS Ningún grupo de seguridad debe permitir el acceso sin restricciones a puertos conocidos, como SSH y Windows protocolo de escritorio remoto (RDP). Para el tráfico entrante, en sus grupos de seguridad, permita únicamente las conexiones TCP o UDP en los puertos autorizados. Para conectarse a instancias de Amazon Elastic Compute Cloud (Amazon EC2), utilice Session Manager o Run Command en lugar del acceso directo por SSH o RDP.

Para obtener más información, consulte los siguientes recursos:

- Trabaja con grupos de seguridad en la EC2 documentación de Amazon
- Controle el tráfico a sus AWS recursos mediante los grupos de seguridad de la documentación de Amazon VPC

Bloquear el acceso público a los documentos de Systems Manager

A menos que su caso de uso requiera que esté activada la compartición pública, las prácticas AWS Systems Manager recomendadas recomiendan bloquear la compartición pública de los documentos de Systems Manager. El uso compartido público puede proporcionar un acceso no deseado a los documentos. Un documento público de Systems Manager puede exponer información valiosa y confidencial sobre su cuenta, sus recursos y sus procesos internos.

Para obtener más información, consulte los siguientes recursos:

- Mejores prácticas para los documentos de Systems Manager compartidos en la documentación de Systems Manager
- Modificar los permisos de un documento compartido de Systems Manager en la documentación de Systems Manager

Bloquear el acceso público a las funciones de Lambda

AWS Lambda es un servicio de computación que ayuda a ejecutar código sin necesidad de aprovisionar ni administrar servidores. Las funciones Lambda no deben ser de acceso público, ya que esto podría permitir el acceso no deseado al código de la función.

Le recomendamos que configure políticas basadas en recursos para que las funciones de Lambda denieguen el acceso desde fuera de su cuenta. Para ello, puede eliminar los permisos o añadir la `AWS:SourceAccount` condición a la declaración que permite el acceso. Puede actualizar las políticas basadas en recursos para las funciones de Lambda a través de la API de Lambda o (). AWS Command Line Interface AWS CLI

También le recomendamos que habilite la función [Lambda.1] Las políticas de la función Lambda deberían prohibir el control de acceso público en. AWS Security Hub Este control valida que las políticas basadas en recursos para las funciones de Lambda prohíben el acceso público.

Para obtener más información, consulte los siguientes recursos:

- AWS Lambda controles en la documentación de Security Hub
- Uso de políticas basadas en recursos para Lambda en la documentación de Lambda
- Recursos y condiciones para las acciones de Lambda en la documentación de Lambda

Restrinja el tráfico entrante y saliente en el grupo de seguridad predeterminado

Si no asocias un grupo de seguridad personalizado al aprovisionar un AWS recurso, el recurso se asocia al grupo de seguridad predeterminado de la VPC. Las reglas predeterminadas de este grupo de seguridad permiten todo el tráfico entrante de todos los recursos asignados a este grupo de seguridad, así como todo el tráfico saliente IPv4 . IPv6 Esto podría permitir el tráfico no deseado hacia el recurso.

AWS recomienda no utilizar el grupo de seguridad predeterminado. En su lugar, cree grupos de seguridad personalizados para recursos o grupos de recursos específicos.

Como el grupo de seguridad predeterminado no se puede eliminar, le recomendamos que cambie las reglas del grupo de seguridad predeterminado para restringir el tráfico entrante y saliente. Al configurar las reglas de los grupos de seguridad, siga el principio del privilegio mínimo.

También le recomendamos que habilite la VPC [EC2.2] Los grupos de seguridad predeterminados no deben permitir el control del tráfico entrante o saliente en Security Hub. Este control valida que el grupo de seguridad predeterminado de una VPC deniegue el tráfico entrante y saliente.

Para obtener más información, consulte los siguientes recursos:

- Controle el tráfico a sus AWS recursos mediante los grupos de seguridad de la documentación de Amazon VPC
- Grupos de seguridad predeterminados para usted VPCs en la documentación de Amazon VPC
- EC2Controles de Amazon en la documentación de Security Hub

Escanee en busca de vulnerabilidades de software y de exposición no intencionada a la red

Te recomendamos que habilites Amazon Inspector en todas tus cuentas. Amazon Inspector es un servicio de administración de vulnerabilidades que analiza continuamente las EC2 instancias de Amazon, las imágenes de contenedores del Amazon Elastic Container Registry (Amazon ECR) y las funciones de Lambda para detectar vulnerabilidades de software y exposiciones no intencionadas en la red. También admite la inspección exhaustiva de las EC2 instancias de Amazon. Cuando Amazon Inspector identifica una vulnerabilidad o una ruta de red abierta, produce un hallazgo que usted puede investigar. Si Amazon Inspector y Security Hub están configurados en tu cuenta, Amazon Inspector envía automáticamente los resultados de seguridad a Security Hub para su administración centralizada.

Para obtener más información, consulte los siguientes recursos:

- Escaneo de recursos con Amazon Inspector en la documentación de Amazon Inspector
- Amazon Inspector: Inspección exhaustiva de Amazon EC2 en la documentación de Amazon Inspector
- Escanea EC2 AMIs con Amazon Inspector en el blog AWS de seguridad
- Elaboración de un programa escalable de gestión de vulnerabilidades basado AWS en AWS Prescriptive Guidance
- Automatice la protección de la red en AWS Well-Architected Framework
- Automatice la protección informática en AWS Well-Architected Framework

Configure AWS WAF

AWS WAFes un firewall de aplicaciones web que le ayuda a supervisar y bloquear las solicitudes HTTP o HTTPS que se reenvían a los recursos de aplicaciones web protegidas, como Amazon API Gateway APIs, CloudFront las distribuciones de Amazon o los balanceadores de carga de aplicaciones. Según los criterios que especifique, el servicio responde a las solicitudes con el contenido solicitado, con un código de estado HTTP 403 (prohibido) o con una respuesta personalizada. AWS WAF puede ayudar a proteger las aplicaciones web o APIs contra las vulnerabilidades web más comunes que pueden afectar a la disponibilidad, comprometer la seguridad o consumir recursos excesivos. Considere la posibilidad de configurar AWS WAF Cuentas de AWS y utilizar una combinación de reglas AWS administradas, reglas personalizadas e integraciones de socios para ayudar a proteger sus aplicaciones de los ataques en la capa de aplicación (capa 7).

Para obtener más información, consulte los siguientes recursos:

- Para empezar, consulte AWS WAF la documentación AWS WAF
- AWS WAF socios de entrega en el AWS sitio web
- Automatizaciones de seguridad para AWS WAF la biblioteca de AWS soluciones
- Implemente la inspección y la protección en el marco de AWS Well-Architected

Configure protecciones avanzadas contra los ataques S DDo

AWS Shieldproporciona protección contra los ataques de denegación de servicio (DDoS) distribuidos contra AWS los recursos de las capas de red y transporte (capas 3 y 4) y la capa de aplicaciones (capa 7). Este servicio está disponible en dos opciones: AWS Shield Standard y AWS Shield Advanced. Shield Standard protege automáticamente AWS los recursos compatibles, sin coste adicional.

Le recomendamos que se suscriba a Shield Advanced, que proporciona una protección ampliada contra ataques DDo S para recursos protegidos. Las protecciones que recibe de Shield Advanced varían en función de la arquitectura y las opciones de configuración. Considere la posibilidad de implementar las protecciones Shield Advanced para las aplicaciones en las que necesite alguno de los siguientes requisitos:

- Disponibilidad garantizada para los usuarios de la aplicación.

- Acceso rápido a expertos en mitigación DDo S si la aplicación se ve afectada por un ataque DDo S.
- Conciencia por parte de AWS de que la aplicación podría verse afectada por un ataque DDo tipo S y notificación de los ataques por parte de AWS y su intensificación a sus equipos de seguridad u operaciones.
- Los costes de la nube son predecibles, incluso si un ataque DDo tipo S afecta al uso de Servicios de AWS.

Para obtener más información, consulte los siguientes recursos:

- AWS Shield Advanced información general en la documentación de Shield
- AWS Shield Advanced recursos protegidos en la documentación de Shield
- AWS Shield Advanced capacidades y opciones en la documentación de Shield
- Respuesta a los eventos DDo S en la documentación de Shield
- Implemente la inspección y la protección en el marco de AWS Well-Architected

Utilice un defense-in-depth enfoque para controlar el tráfico de la red

AWS Network Firewall es un firewall de red gestionado y con estado y un servicio de detección y prevención de intrusiones para nubes privadas virtuales (VPCs) en el. Nube de AWS Le ayuda a implementar protecciones de red esenciales en el perímetro de la VPC. Esto incluye filtrar el tráfico que entra y viene de una puerta de enlace de Internet, una puerta de enlace NAT o a través de una VPN o AWS Direct Connect. Network Firewall incluye funciones que ayudan a proteger contra las amenazas de red más comunes. El firewall con estado de Network Firewall puede incorporar el contexto de los flujos de tráfico, como las conexiones y los protocolos, para hacer cumplir las políticas.

Para obtener más información, consulte los siguientes recursos:

- AWS Network Firewall documentación
- Controle el tráfico en todos los niveles del AWS Well-Architected Framework

Recomendaciones de control de seguridad para proteger los datos

El AWS Well-Architected Framework agrupa las mejores prácticas para proteger los datos en tres categorías: clasificación de los datos, protección de los datos en reposo y protección de los datos en tránsito. Los controles de seguridad de esta sección pueden ayudarle a implementar las mejores prácticas de protección de datos. Estas prácticas recomendadas fundamentales deben estar implementadas antes de diseñar cualquier carga de trabajo en la nube. Evitan el mal manejo de los datos y le ayudan a cumplir con las obligaciones organizativas, reglamentarias y de cumplimiento. Utilice los controles de seguridad de esta sección para implementar las mejores prácticas de protección de datos.

Controles de esta sección:

- Identifique y clasifique los datos a nivel de carga de trabajo
- Establezca controles para cada nivel de clasificación de datos
- Cifre los datos en reposo
- Cifre los datos en tránsito
- Bloquear el acceso público a las instantáneas de Amazon EBS
- Bloquear el acceso público a las instantáneas de Amazon RDS
- Bloquear el acceso público a Amazon RDS, Amazon Redshift y los recursos AWS DMS
- Bloquear el acceso público a los buckets de Amazon S3
- Exija a MFA que elimine los datos de los buckets críticos de Amazon S3
- Configurar los dominios OpenSearch de Amazon Service en una VPC
- Configure las alertas para su eliminación AWS KMS key
- Bloquee el acceso público a AWS KMS keys
- Configure los detectores del balanceador de carga para que usen protocolos seguros

Identifique y clasifique los datos a nivel de carga de trabajo

La clasificación de datos es un proceso para identificar y clasificar los datos de su red en función de su importancia y sensibilidad. Es un componente fundamental de cualquier estrategia de administración de riesgos de ciberseguridad porque lo ayuda a determinar los controles de

protección y retención adecuados para los datos. La clasificación de los datos a menudo reduce la frecuencia de la duplicación de los datos. Esto puede reducir los costos de almacenamiento y respaldo y acelerar las búsquedas.

Le recomendamos que comprenda el tipo y la clasificación de los datos que procesa su carga de trabajo, los procesos empresariales asociados, dónde se almacenan los datos y quién es el propietario de los datos. La clasificación de datos ayuda a los propietarios de la carga de trabajo a identificar las ubicaciones que almacenan datos confidenciales y a determinar cómo se debe acceder a esos datos y compartirlos. Las etiquetas son pares clave-valor que actúan como metadatos para organizar los AWS recursos. Las etiquetas pueden ayudar a administrar, identificar, organizar, buscar y filtrar los recursos.

Para obtener más información, consulte los siguientes recursos:

- Clasificación de datos en documentos AWS técnicos
- Identifique los datos de su carga de trabajo en AWS Well-Architected Framework

Establezca controles para cada nivel de clasificación de datos

Defina los controles de protección de datos para cada nivel de clasificación. Por ejemplo, utilice los controles recomendados para proteger los datos clasificados como públicos y proteja los datos confidenciales con controles adicionales. Utilice mecanismos y herramientas que reduzcan o eliminen la necesidad de acceder directamente a los datos o de procesarlos manualmente. La automatización de la identificación y clasificación de los datos reduce el riesgo de errores de clasificación, manipulación, modificación o error humano.

Por ejemplo, considere la posibilidad de utilizar Amazon Macie para escanear los depósitos del Amazon Simple Storage Service (Amazon S3) en busca de datos confidenciales, como información de identificación personal (PII). Además, puede automatizar la detección del acceso no deseado a los datos mediante los registros de flujo de VPC en Amazon Virtual Private Cloud (Amazon VPC).

Para obtener más información, consulte los siguientes recursos:

- Defina los controles de protección de datos en el AWS Well-Architected Framework
- Automatice la identificación y la clasificación en el marco de AWS Well-Architected
- AWS La arquitectura de referencia de privacidad (AWS PRA) en AWS la guía prescriptiva
- Descubrimiento de datos confidenciales con Amazon Macie en la documentación de Macie

- Registro del tráfico IP mediante los registros de flujo de VPC en la documentación de Amazon VPC
- Se utilizan técnicas habituales para detectar datos de PHI y PII Servicios de AWS en el AWS blog for Industries

Cifre los datos en reposo

Los datos en reposo son datos estacionarios en la red, como los datos almacenados. La implementación del cifrado y los controles de acceso adecuados para los datos en reposo ayudan a reducir el riesgo de acceso no autorizado. El cifrado es un proceso informático que transforma los datos de texto plano, legibles por humanos, en texto cifrado. Necesita una clave de cifrado para volver a descifrar el contenido en texto sin formato para que pueda usarse. En el Nube de AWS, puede usar AWS Key Management Service (AWS KMS) para crear y controlar claves criptográficas que ayuden a proteger sus datos.

Como se explica enEstablezca controles para cada nivel de clasificación de datos, recomendamos crear una política que especifique qué tipo de datos deben cifrarse. Incluya criterios sobre cómo determinar qué datos deben cifrarse y qué datos deben protegerse con otra técnica, como la tokenización o el uso de hash.

Para obtener más información, consulte los siguientes recursos:

- Configuración del cifrado predeterminado en la documentación de Amazon S3
- Cifrado predeterminado para los nuevos volúmenes de EBS y copias instantáneas en la documentación de Amazon EC2
- Cifrado de los recursos de Amazon Aurora en la documentación de Amazon Aurora
- Introducción a los detalles criptográficos de AWS KMS la documentación AWS KMS
- Cómo crear una estrategia empresarial de cifrado para los datos almacenados en AWS Prescriptive Guidance
- Aplique el cifrado en reposo en el marco AWS Well-Architected
- Para obtener más información sobre el cifrado en concreto Servicios de AWS, consulte la AWS documentación de ese servicio

Cifre los datos en tránsito

Los datos en tránsito son datos que se mueven de forma activa por la red, por ejemplo, entre los recursos de la red. Cifre todos los datos en tránsito mediante protocolos y conjuntos de cifrado TLS seguros. El tráfico de red entre los recursos e Internet debe estar cifrado para evitar el acceso no autorizado a los datos. Siempre que sea posible, utilice TLS para cifrar el tráfico de red en su entorno interno AWS .

Para obtener más información, consulte los siguientes recursos:

- Exigir HTTPS para la comunicación entre los espectadores y CloudFront en la CloudFront documentación de Amazon
- Documentación de AWS PrivateLink
- Imponga el cifrado en tránsito en el AWS Well-Architected Framework
- Para obtener más información sobre el cifrado en concreto Servicios de AWS, consulte la AWS documentación de ese servicio

Bloquear el acceso público a las instantáneas de Amazon EBS

Amazon Elastic Block Store (Amazon EBS) proporciona volúmenes de almacenamiento a nivel de bloques para utilizarlos con instancias de Amazon Elastic Compute Cloud (Amazon). EC2 Puede realizar copias de seguridad de los datos de sus volúmenes de Amazon EBS en Amazon S3 realizando point-in-time instantáneas. Puede compartir las instantáneas públicamente con todos los demás Cuentas de AWS o puede compartirlas de forma privada con la persona Cuentas de AWS que especifique.

Le recomendamos que no comparta públicamente las instantáneas de Amazon EBS. Esto podría exponer datos confidenciales de forma inadvertida. Cuando compartes una instantánea, permites que otras personas accedan a los datos de la instantánea. Comparta las instantáneas solo con personas en las que confíe todos estos datos.

Para obtener más información, consulte los siguientes recursos:

- Comparte una instantánea en la EC2 documentación de Amazon
- Las instantáneas de Amazon EBS no deberían poder restaurarse públicamente en la documentación AWS Security Hub

- ebs-snapshot-public-restorable-consulte la documentación AWS Config

Bloquear el acceso público a las instantáneas de Amazon RDS

Amazon Relational Database Service (Amazon RDS) le ayuda a configurar, operar y escalar una base de datos relacional en. Nube de AWS Amazon RDS crea y guarda copias de seguridad automatizadas de la instancia de base de datos (DB) o del clúster de base de datos Multi-AZ durante el período de copia de seguridad de la instancia de base de datos. Amazon RDS crea una instantánea del volumen de almacenamiento de la instancia de base de datos; para ello, hace una copia de seguridad de toda la instancia de base de datos y no solo de las bases de datos individuales. Puede compartir una instantánea manual con el fin de copiarla o restaurar una instancia de base de datos a partir de ella.

Si comparte una instantánea como pública, asegúrese de que ninguno de los datos de la instantánea sea privado o confidencial. Cuando una instantánea se comparte públicamente, todos los Cuentas de AWS permisos necesarios para acceder a los datos. Esto puede provocar una exposición no intencionada de los datos de su instancia de Amazon RDS.

Para obtener más información, consulte los siguientes recursos:

- Compartir una instantánea de base de datos en la documentación de Amazon RDS
- rds-snapshots-public-prohibitedden la documentación AWS Config
- La instantánea de RDS debe ser privada en la documentación de Security Hub

Bloquear el acceso público a Amazon RDS, Amazon Redshift y los recursos AWS DMS

Puede configurar las instancias de base de datos de Amazon RDS, los clústeres de Amazon Redshift AWS Database Migration Service y las instancias de AWS DMS() replicación para que sean de acceso público. Si el valor del `publiclyAccessible` campo es`true`, estos recursos son de acceso público. Permitir el acceso público puede provocar tráfico innecesario, exposición o filtraciones de datos. Le recomendamos que no permita el acceso público a estos recursos.

Le recomendamos que habilite AWS Config reglas o controles de Security Hub para detectar si las instancias de base de datos de Amazon RDS, las instancias de AWS DMS replicación o los clústeres de Amazon Redshift permiten el acceso público.

> **Note**
>
> La configuración de acceso público de las instancias de AWS DMS replicación no se puede modificar una vez aprovisionada la instancia. Para cambiar la configuración de acceso público, elimine la instancia actual y, a continuación, vuelva a crearla. Cuando la vuelvas a crear, no selecciones la opción de acceso público.

Para obtener más información, consulte los siguientes recursos:

- AWS DMS las instancias de replicación no deben ser públicas en la documentación de Security Hub
- Las instancias de base de datos de RDS deberían prohibir el acceso público en la documentación de Security Hub
- Los clústeres de Amazon Redshift deberían prohibir el acceso público en la documentación de Security Hub
- rds-instance-public-access-consulte la documentación AWS Config
- dms-replication-not-publicen la documentación AWS Config
- redshift-cluster-public-access-consulte la documentación AWS Config
- Modificación de una instancia de base de datos de Amazon RDS en la documentación de Amazon RDS
- Modificación de un clúster en la documentación de Amazon Redshift

Bloquear el acceso público a los buckets de Amazon S3

Es una práctica recomendada de seguridad de Amazon S3 garantizar que sus buckets no sean de acceso público. A menos que exijas explícitamente a cualquier usuario de Internet que pueda leer o escribir en tu bucket, asegúrate de que tu bucket no sea público. Esto ayuda a proteger la integridad y la seguridad de los datos. Puede utilizar AWS Config las reglas y los controles de Security Hub para confirmar que sus buckets de Amazon S3 cumplen con esta práctica recomendada.

Para obtener más información, consulte los siguientes recursos:

- Prácticas recomendadas de seguridad de Amazon S3 en la documentación de Amazon S3

- La configuración S3 Block Public Access debe estar habilitada en la documentación del Security Hub
- Los buckets S3 deberían prohibir el acceso público de lectura en la documentación del Security Hub
- Los buckets S3 deberían prohibir el acceso público de escritura en la documentación del Security Hub
- bucket-public-read-prohibited regla s3- en la documentación AWS Config
- s3- bucket-public-write-prohibited en la AWS Config documentación

Exija a MFA que elimine los datos de los buckets críticos de Amazon S3

Cuando se trabaja con S3 Versioning en buckets de Amazon S3, puede agregar de forma opcional otra capa de seguridad al configurar un bucket para habilitar la eliminación con MFA (autenticación multifactor). Si lo hace, el propietario del bucket debe incluir dos formas de autenticación en cualquier solicitud para eliminar una versión o cambiar el estado de control de versiones del bucket. Le recomendamos que habilite esta función para los depósitos que contienen datos críticos para su organización. Esto puede evitar la eliminación accidental de cubos y datos.

Para obtener más información, consulte los siguientes recursos:

- Configuración de la eliminación de MFA en la documentación de Amazon S3

Configurar los dominios OpenSearch de Amazon Service en una VPC

Amazon OpenSearch Service es un servicio gestionado que te ayuda a implementar, operar y escalar OpenSearch clústeres en Nube de AWS. Amazon OpenSearch Service apoya OpenSearch y legado Elasticsearch software de código abierto (OSS). Los dominios de Amazon OpenSearch Service que se implementan en una VPC pueden comunicarse con los recursos de la VPC a través de la AWS red privada, sin necesidad de atravesar la Internet pública. Esta configuración mejora su nivel de seguridad al restringir el acceso a los datos en tránsito. Le recomendamos que no adjunte dominios de Amazon OpenSearch Service a subredes públicas y que la VPC se configure de acuerdo con las prácticas recomendadas.

Para obtener más información, consulte los siguientes recursos:

- Cómo lanzar tus dominios OpenSearch de Amazon Service dentro de una VPC en la documentación de Amazon OpenSearch Service
- opensearch-in-vpc-onlyen la documentación AWS Config
- OpenSearch los dominios deben estar en una VPC en la documentación de Security Hub

Configure las alertas para su eliminación AWS KMS key

AWS Key Management Service (AWS KMS) las claves no se pueden recuperar una vez eliminadas. Si se elimina una clave de KMS, los datos que aún estén cifrados con esa clave no se podrán recuperar de forma permanente. Si necesita conservar el acceso a los datos, antes de eliminar la clave, debe descifrar los datos o volver a cifrarlos con una clave KMS nueva. Debe eliminar una clave KMS solo cuando esté seguro de que ya no necesita usarla.

Le recomendamos que configure una CloudWatch alarma de Amazon que le notifique si alguien inicia la eliminación de una clave de KMS. Dado que eliminar una clave de KMS es destructivo y potencialmente peligroso, es AWS KMS necesario establecer un período de espera y programar la eliminación en 7 a 30 días. Esto brinda la oportunidad de revisar la eliminación programada y cancelarla, si es necesario.

Para obtener más información, consulte los siguientes recursos:

- Programar y cancelar la eliminación de claves en la documentación AWS KMS
- Crear una alarma que detecte el uso de una clave KMS pendiente de ser eliminada en la documentación AWS KMS
- AWS KMS keys no debe eliminarse involuntariamente en la documentación del Security Hub

Bloquee el acceso público a AWS KMS keys

Las políticas clave son la forma principal de controlar el acceso a AWS KMS keys. Cada clave KMS tiene exactamente una política de claves. Permitir el acceso anónimo a las claves de KMS puede provocar una filtración de datos confidenciales. Le recomendamos que identifique todas las claves de KMS de acceso público y actualice sus políticas de acceso para evitar que se envíen solicitudes no firmadas a estos recursos.

Para obtener más información, consulte los siguientes recursos:

- Las prácticas recomendadas de seguridad se encuentran AWS Key Management Service en la documentación AWS KMS
- Cambiar una política clave en la AWS KMS documentación
- Determinar el acceso AWS KMS keys a la AWS KMS documentación

Configure los detectores del balanceador de carga para que usen protocolos seguros

Elastic Load Balancing distribuye automáticamente el tráfico entrante de las aplicaciones entre varios destinos. Puede configurar el equilibrador de carga para que acepte el tráfico entrante especificando uno o varios oyentes. Un oyente es un proceso que comprueba las solicitudes de conexión utilizando el protocolo y el puerto configurados. Cada tipo de balanceador de carga admite distintos protocolos y puertos:

- Los balanceadores de carga de aplicaciones toman decisiones de enrutamiento en la capa de aplicación y utilizan protocolos HTTP o HTTPS.
- Los balanceadores de carga de red toman las decisiones de enrutamiento en la capa de transporte y utilizan los protocolos TCP, TLS, UDP o TCP_UDP.
- Los balanceadores de carga clásicos toman las decisiones de enrutamiento en la capa de transporte (mediante protocolos TCP o SSL) o en la capa de aplicación (mediante protocolos HTTP o HTTPS).

Te recomendamos que utilices siempre los protocolos HTTPS o TLS. Estos protocolos garantizan que el equilibrador de carga sea responsable de cifrar y descifrar el tráfico entre el cliente y el destino.

Para obtener más información, consulte los siguientes recursos:

- Listeners para tus balanceadores de carga de aplicaciones en la documentación de Elastic Load Balancing
- Listeners para tu Classic Load Balancer en la documentación de Elastic Load Balancing
- Listeners para sus balanceadores de carga de red en la documentación de Elastic Load Balancing
- Asegúrese de que los balanceadores de AWS carga utilicen protocolos de escucha seguros en la Guía prescriptiva AWS

- elb-tls-https-listeners-solo en la documentación AWS Config
- Los oyentes de Classic Load Balancer deben configurarse con una terminación HTTPS o TLS en la documentación de Security Hub
- El Application Load Balancer debe configurarse para redirigir todas las solicitudes HTTP a HTTPS en la documentación de Security Hub

Recomendaciones de seguridad para responder a los incidentes

Cuando se produce un incidente de seguridad en su organización, los usuarios deben estar preparados para responder al problema. Todos los usuarios deben tener un conocimiento básico de los procesos de respuesta de seguridad de su organización. La planificación, la formación y la experiencia son fundamentales para el éxito de un programa de respuesta a incidentes. Lo ideal es que prepare a su organización antes de que se produzca un posible incidente de seguridad. El AWS Well-Architected Framework identifica tres bases que se requieren para un programa exitoso de respuesta a incidentes en la nube: preparación, operaciones y actividad posterior al incidente. Para obtener más información, consulte Aspectos de la respuesta a AWS incidentes en AWS Well-Architected Framework.

Con la excepción de los controles de seguridad que le notifican los eventos o responden automáticamente a ellos, hay controles limitados que puede establecer para responder a los incidentes. Una postura sólida de respuesta a los incidentes se establece principalmente a través de los planes, procesos, manuales, manuales y programas de formación que utilice en su organización. Puede utilizar los controles y las recomendaciones de esta sección para implementar las mejores prácticas en su programa de respuesta a incidentes. Para obtener más información sobre las prácticas recomendadas para la respuesta a incidentes y la guía de implementación, consulte Respuesta a incidentes en el AWS Well-Architected Framework.

Recomendaciones de esta sección:

- Defina un plan de respuesta a incidentes
- Cree y mantenga manuales y manuales de respuesta a incidentes
- Implemente la automatización de la seguridad basada en eventos
- Documente cómo deben interactuar los equipos operativos con Soporte
- Configure alertas para eventos de seguridad

Defina un plan de respuesta a incidentes

Establezca un plan de respuesta a incidentes (IRP) bien definido. El plan de respuesta a incidentes está diseñado para ser la base de su programa de respuesta a incidentes. Este plan debe personalizarse para abordar las necesidades de cada organización.

Para obtener más información, consulte los siguientes recursos:

- Desarrolle y pruebe un plan de respuesta a incidentes en la Guía de respuesta a incidentes de AWS seguridad
- Desarrolle planes de gestión de incidentes en el AWS Well-Architected Framework
- Identifique el personal clave y los recursos externos en el AWS Well-Architected Framework

Cree y mantenga manuales y manuales de respuesta a incidentes

Una parte clave de la preparación de los procesos de respuesta a un incidente es la elaboración de manuales. Los manuales de respuesta a incidentes proporcionan una serie de pasos recomendados que los usuarios deben seguir cuando se produce un incidente de seguridad. Tener una estructura y unos pasos claros simplifica la respuesta y reduce la probabilidad de que se produzca un error humano.

Para obtener más información, consulte los siguientes recursos:

- Para qué se pueden crear manuales de estrategias en la Guía de respuesta a incidentes AWS de seguridad
- AWS ejemplos de manuales de respuesta a incidentes sobre GitHub
- Desarrolle y pruebe manuales de respuesta a incidentes de seguridad en el AWS Well-Architected Framework

Implemente la automatización de la seguridad basada en eventos

La automatización de la respuesta de seguridad es 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 preventivos 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.

Muchas Servicios de AWS admiten respuestas automatizadas. Por ejemplo, puedes configurar una CloudWatch alarma de Amazon para métricas específicas y la alarma puede iniciar una acción cuando la alarma cambia de estado. A través de Amazon EventBridge, también puedes configurar la respuesta automática y la corrección de los hallazgos en AWS Security Hub Amazon Inspector.

Para obtener más información, consulta los siguientes recursos:

- Corrija automáticamente los hallazgos de seguridad de Amazon Inspector en el blog AWS de seguridad
- Comience con la automatización de las respuestas de seguridad AWS en el blog de AWS seguridad
- La respuesta de seguridad automatizada está AWS disponible en la biblioteca de AWS soluciones
- Uso de CloudWatch las alarmas de Amazon en la CloudWatch documentación
- Respuesta y corrección automatizadas en la documentación de Security Hub
- Creación de respuestas personalizadas a las conclusiones de Amazon Inspector con Amazon EventBridge en la documentación de Amazon Inspector

Documente cómo deben interactuar los equipos operativos con Soporte

Para usted Cuenta de AWS, puede definir un contacto principal y tres contactos alternativos. Le recomendamos que proporcione un contacto de seguridad para cada uno de ellos Cuenta de AWS o para su organización.

AWS Support ofrece una gama de planes que proporcionan acceso a herramientas y conocimientos que pueden respaldar el éxito y el buen estado operativo de AWS las soluciones. Además, considere si su organización se beneficiaría si utilizara un Soporte plan AWS Managed Services en lugar de uno. AWS Managed Services (AMS) lo ayuda a operar de manera más eficiente y segura al proporcionar una administración continua de su AWS infraestructura, que incluye monitoreo, administración de incidentes, orientación de seguridad, soporte de parches y respaldo para AWS las cargas de trabajo. El modelo de soporte de AMS puede ser más adecuado para las organizaciones que tienen recursos limitados en sus equipos de operaciones en la nube. Le recomendamos que compare estos modelos y planes para elegir el que mejor se adapte al caso de uso de su organización y al nivel de madurez de la nube.

Para obtener más información, consulte los siguientes recursos:

- Conozca los equipos de AWS respuesta y el soporte en la Guía de respuesta a incidentes de AWS seguridad
- Actualice sus contactos alternativos Cuenta de AWS en la Guía de administración de AWS cuentas

- Compare Soporte los planes en el AWS sitio web
- La estrategia que se puede utilizar AWS Managed Services para lograr los resultados comerciales objetivo en la AWS guía prescriptiva

Configure alertas para eventos de seguridad

La detección de una anomalía es tan importante como las medidas implementadas para controlarla. Una alerta es el componente principal de la fase de detección. Genera una notificación para iniciar el proceso de respuesta al incidente en función de Cuenta de AWS la actividad de interés. Asegúrese de que las alertas incluyan información relevante para que el equipo tome medidas.

Para obtener más información, consulte los siguientes recursos:

- La detección en la guía de respuesta a incidentes de AWS seguridad
- Prepare las capacidades forenses en el marco de AWS Well-Architected
- Implemente eventos de seguridad procesables en el AWS Well-Architected Framework

Pasos a seguir a continuación

A medida que continúe su transición a la nube, es importante aplicar estos controles, directrices y opciones de corrección documentados. Estas recomendaciones ayudan a mejorar su postura de seguridad en la nube y a cumplir con sus responsabilidades de seguridad en el modelo de responsabilidad compartida Nube de AWS, tal como se define en el modelo de responsabilidad AWS compartida.

Para los próximos pasos, recomendamos lo siguiente:

- Para obtener más información sobre las mejores prácticas y la guía de implementación, revise los seis pilares del AWS Well-Architected Framework.
- Para los Servicios de AWS que utiliza su organización, revise la lista de AWS Security Hub controles disponibles y evalúe si debe habilitar alguno de estos controles en su entorno.
- Para las Servicios de AWS que usa su organización, revise la lista de reglas AWS Config administradas disponibles y evalúe si debe habilitar alguna de estas reglas en su entorno.

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
MFA para usuario root	Actualizamos las recomendaciones y proporcionamos más información en la sección de MFA para el usuario root.	9 de noviembre de 2023
Publicación inicial	—	27 de octubre de 2023

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 administración y gobierno centralizados.

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de 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 deriva

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 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 suelen realizarse 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 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 keyloggers.

servicios gestionados

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

sistema de ejecución de fabricación (MES)

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

cuenta de miembro

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

MES

Consulte el sistema de ejecución de la fabricación.

Transporte 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 las Revisiones de preparación operativa (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`, normalmente, se encuentra en una cláusula. `WHERE`

pulsar un predicado

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

control preventivo

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

entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz 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 no conformes. Estos controles escanean los recursos antes de aprovisionarlos. Si el recurso no cumple con el control, significa que no está aprovisionado. Para obtener más información, consulte la guía de referencia de controles en la AWS Control Tower documentación y consulte Controles proactivos en Implementación de controles de seguridad en AWS.

gestión del ciclo de vida del producto (PLM)

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

entorno de producción

Consulte el entorno.

controlador lógico programable (PLC)

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

encadenamiento rápido

Utilizar la salida de una solicitud de LLM como entrada para la siguiente solicitud 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 Recuperación y generación aumentada.

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 e independiente de los demás para proporcionar tolerancia a las fallas, estabilidad y resiliencia. Para obtener más información, consulte Regiones de AWS Especificar qué cuenta puede usar.

regresión

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

volver a alojar

Consulte 7 Rs.

versión

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

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

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. Nube de AWS

SPOT

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.

Emparejamiento de 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 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.