Implementación de controles de seguridad en AWS

AWS Guía prescriptiva

AWS Guía prescriptiva: Implementación de controles de seguridad en AWS

Table of Contents

Introducción 1
Destinatarios previstos 1
Resultados empresariales específicos 3
Controles de seguridad en el marco de gobernanza 4
Tipos de controles de seguridad 6
Controles preventivos 6
Objetivos 7
Proceso 8
Casos de uso 8
Tecnología 9
Resultados empresariales 10
Controles proactivos 10
Objetivos 11
Proceso 12
Casos de uso 12
Tecnología 13
Resultados empresariales 13
Controles de detección 14
Objetivos 15
Proceso 15
Casos de uso 15
Tecnología 16
Resultados empresariales 19
Controles de respuesta 20
Objetivos 20
Proceso 20
Casos de uso 21
Tecnología 21
Resultados empresariales 22
Siguientes pasos 23
Preguntas frecuentes 24
¿En qué debo enfocarme si tengo tiempo y recursos limitados y no puedo implementar todos estos tipos de controles? 24
Recursos 25

Documentación de AWS 25
Publicaciones de blog de AWS 25
Otros recursos 25
Historial del documento 26
Glosario 27
..... 27
A 28
B 31
C 33
D 36
E 41
F 43
G 44
H 45
I 46
L 49
M 50
O 54
P 57
Q 60
R 60
S 63
T 67
U 68
V 69
W 69
Z 70
..... lxxii

Implementación de controles de seguridad en AWS

Iqbal Umair, Gurpreet Kaur Cheema, Wasim Hossain, Joseph Nguyen, San Brar y Lucia Vanta, Amazon Web Services (AWS)

Diciembre de 2023 (historial de documentos)

La seguridad es fundamental para todas las empresas y es un pilar clave en el Marco de AWS Well-Architected. Sin embargo, muchos no saben cómo abordar las consideraciones de seguridad y crear una estrategia integral y automatizada de pruebas y corrección de seguridad para sus entornos en la nube. Mediante el uso de herramientas y Servicios de AWS, como AWS Config, Amazon GuardDuty y AWS CloudFormation, puede crear una estrategia de pruebas de seguridad e incorporarla a su entorno en la Nube de AWS.

A fin de ayudar a cumplir con las políticas y los estándares de seguridad de su empresa, los controles de seguridad son las barreras de protección técnicas o administrativas que ayudan a prevenir, detectar o reducir la capacidad de un agente de amenazas para aprovechar una vulnerabilidad de seguridad. Se han diseñado para proteger la confidencialidad, la integridad y la disponibilidad de los recursos y los datos. Los siguientes son ejemplos de controles de seguridad:

- Implementar la autenticación multifactor para los usuarios que necesitan iniciar sesión en una aplicación
- Acciones de consulta, registro y monitoreo con el fin de realizar auditorías en tiempo real de la actividad de la cuenta
- Asegurarse de que los datos confidenciales se encuentren cifrados
- Asegurarse de que los registros se almacenen de acuerdo con la política de retención de su empresa

Existen cuatro tipos de controles de seguridad: preventivos, proactivos, de detección y de respuesta. En esta guía, se describe cada tipo con más detalle y se hace hincapié en cómo implementar y automatizar estos controles en la Nube de AWS. En esta guía, se ofrece ayuda para implementar controles de seguridad que sean continuos y proactivos.

Destinatarios previstos

Esta guía se ha diseñado para arquitectos e ingenieros de seguridad responsables de implementar los controles de seguridad en la Nube de AWS. Si su empresa no ha definido una política de

seguridad, objetivos de control o estándares, como se describe en Controles de seguridad en el marco de gobernanza, le recomendamos que complete estas tareas de gobernanza antes de continuar con esta guía.

Resultados empresariales específicos

Las empresas utilizan los controles de seguridad para mitigar los riesgos de sus sistemas de TI o para actuar como medidas correctivas frente a dichos riesgos. Los controles definen la base de los requisitos para satisfacer los principales objetivos de seguridad de un programa de TI y su estrategia de seguridad. Contar con controles mejora la posición de seguridad de una empresa al proteger la confidencialidad, integridad y disponibilidad de sus datos y activos de TI. Sin controles, sería difícil saber dónde hay que centrarse e invertir para establecer una línea de base de seguridad.

Los controles de seguridad se pueden utilizar para abordar una variedad de escenarios. Los ejemplos incluyen cumplir con los requisitos derivados de las evaluaciones de riesgos, alcanzar los estándares del sector o cumplir con las normativas. Cumplir con los controles de seguridad demuestra que se ha medido el riesgo para un sistema, se ha determinado el nivel de protección necesario y se han implementado soluciones de forma proactiva. Otros factores, como el negocio, la industria y la geografía, pueden determinar los controles de seguridad que necesita.

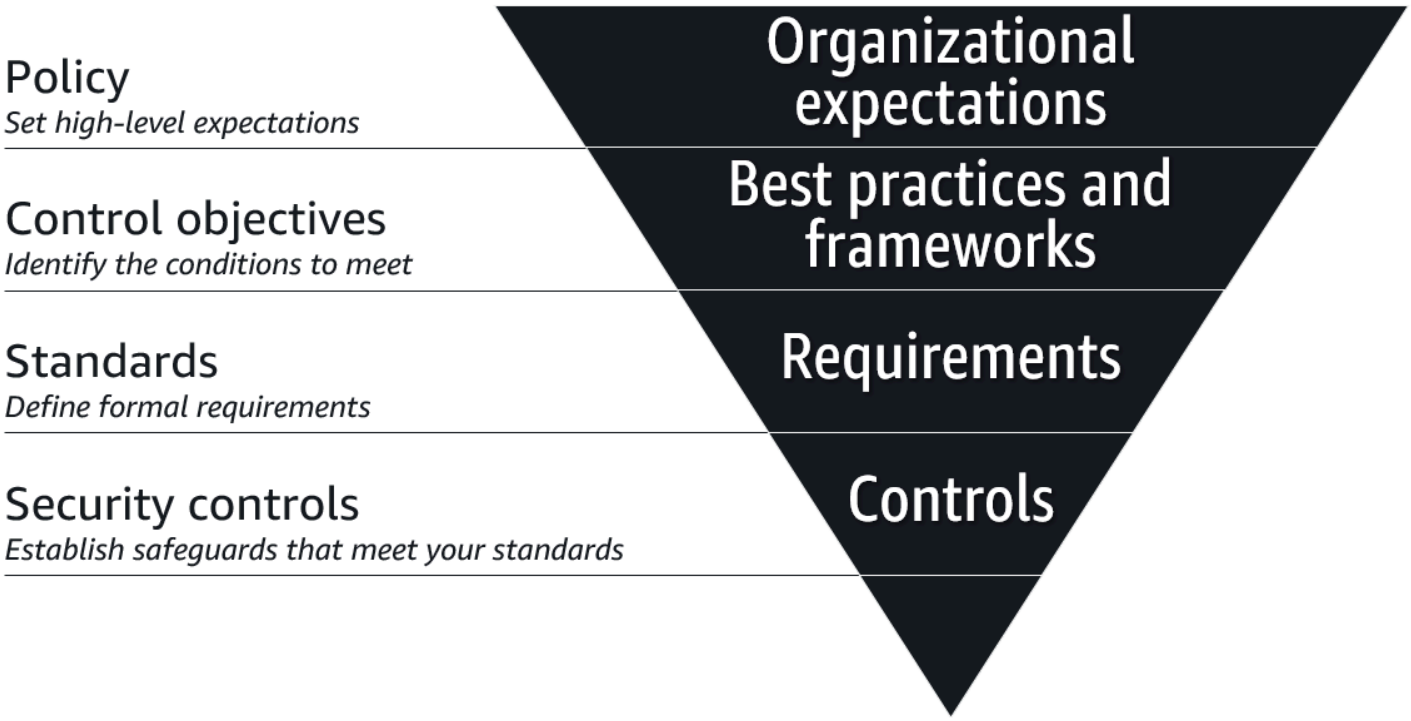
Los siguientes son casos de uso comunes para la implementación de los controles de seguridad:

- En la evaluación de seguridad de una aplicación se ha identificado la necesidad de controles de acceso en función de la confidencialidad de los datos que se procesan.
- Debe cumplir con los estándares de seguridad, como las Normas de seguridad de datos del sector de las tarjetas de pago (PCI DSS), la HIPAA (Ley de Portabilidad y Responsabilidad de Seguros de Salud) o el Instituto Nacional de Estándares y Tecnología (NIST).
- Debe proteger la información confidencial para las transacciones empresariales.
- Su empresa se ha expandido a una región geográfica que requiere controles de seguridad, como una región que exige la conformidad con el Reglamento General de Protección de Datos (RGPD).

Tras leer esta guía, debería estar familiarizado con los cuatro tipos de controles de seguridad, comprender de qué manera forman parte de su marco de gobernanza de seguridad y estar preparado para comenzar a implementar y automatizar los controles de seguridad en la Nube de AWS.

Controles de seguridad en el marco de gobernanza

Es importante planificar desde un nivel básico. ¿Cómo se comienza? En la siguiente figura, se muestra cómo se puede crear una estrategia de gobernanza de la seguridad basada en una política, objetivos de control, estándares y controles de seguridad.



Los siguientes son los componentes jerárquicos de una estrategia de gobernanza de la seguridad:

- Política: una política es la base de cualquier estrategia de gobernanza de ciberseguridad. Es un documento que establece las expectativas de la empresa, como las obligaciones legales, reglamentarias o contractuales que debe cumplir. Las políticas pueden variar en función del sector y la región.
- Objetivos de control: los objetivos de control son metas, como las prácticas recomendadas reconocidas en el sector, que ayudan a cumplir la intención de una política. En el caso de la computación en la nube, muchas empresas adoptan la Matriz de controles en la nube (CCM) (sitio web de Cloud Security Alliance), que es un marco de objetivos de control de ciberseguridad.
- Estándares: los estándares son requisitos que se establecen de manera formal y satisfacen un objetivo de control. Los estándares pueden incluir procesos, acciones o configuraciones, y son cuantificables para que pueda medir el rendimiento en comparación con el estándar.

- Controles de seguridad: los controles de seguridad son los mecanismos técnicos o administrativos que se llevan a cabo para implementar los estándares. Todos los controles de seguridad se ajustan a los estándares, pero no todos los estándares se ajustan a los controles de seguridad. Las pruebas de los controles de seguridad se han diseñado para monitorear y medir si se cumplen de manera efectiva los estándares definidos.

Esta guía se enfoca en cómo diseñar e implementar los tipos comunes de controles de seguridad en la Nube de AWS.

Tipos de controles de seguridad

Existen cuatro tipos de controles de seguridad principales:

- Controles preventivos: estos controles se han diseñado para evitar que ocurra un evento.
- Controles proactivos: estos controles se diseñaron para evitar la creación de recursos que no cumplan con las normas.
- Controles de detección: estos controles se han diseñado para detectar, registrar y alertar después de que se produzca un evento.
- Controles de respuesta: estos controles se han diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad.

Una estrategia de seguridad eficaz incluye los cuatro tipos de controles de seguridad. Los controles preventivos son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Sin embargo, es importante asegurarse de establecer controles de detección y de respuesta a fin de saber cuándo se produce un evento y poder tomar las medidas adecuadas e inmediatas para solucionarlo. El uso de controles proactivos agrega otra capa de seguridad porque complementa a los controles preventivos, que suelen ser de naturaleza más estricta.

En las siguientes secciones, se describe cada tipo de control en más detalle. Se analizan los objetivos, el proceso de implementación, los casos de uso, las consideraciones tecnológicas y los resultados esperados de cada tipo de control.

Controles preventivos

Los controles preventivos son controles de seguridad que se han diseñado para evitar que ocurra un evento. Estas barreras de protección son la primera línea de defensa para evitar el acceso no autorizado o los cambios no deseados en la red. Un ejemplo de control preventivo es un rol AWS Identity and Access Management (IAM) que tiene acceso de solo lectura porque ayuda a evitar acciones de escritura no deseadas por parte de usuarios no autorizados.

Revise la siguiente información acerca de este tipo de controles:

- Objetivos
- Proceso
- Casos de uso

- Tecnología
- Resultados empresariales

Objetivos

El objetivo principal de los controles preventivos es minimizar o evitar la probabilidad de que se produzca una amenaza. El control debe ayudar a evitar el acceso no autorizado al sistema e impedir que los cambios no intencionados afecten al sistema. Los objetivos de los controles preventivos son los siguientes:

- División de funciones: los controles preventivos pueden establecer límites lógicos que restringen los privilegios, de manera de que con los permisos solo se realicen tareas específicas en cuentas o entornos designados. Entre los ejemplos se incluyen:
  - Segmentar las cargas de trabajo en diferentes cuentas para servicios específicos
  - Separar y contabilizar en entornos aislados de producción, desarrollo y pruebas
  - Delegar el acceso y las responsabilidades a varias entidades para que desempeñen funciones específicas, como utilizar roles de IAM o roles asumidos a fin de permitir que solo funciones laborales específicas realicen determinadas acciones
- Control de acceso: los controles preventivos pueden conceder o denegar el acceso a los recursos y datos del entorno de forma sistemática. Entre los ejemplos se incluyen:
  - Impedir que los usuarios superen los permisos previstos, lo que se conoce como escalado de privilegios
  - Restringir el acceso a aplicaciones y datos solo a los usuarios y servicios autorizados
  - Mantener reducido el grupo de administradores
  - Evitar el uso de las credenciales de usuario raíz.
- Cumplimiento: los controles preventivos pueden ayudar a su empresa a cumplir con sus políticas, directrices y estándares. Entre los ejemplos se incluyen:
  - Bloquear configuraciones que sirvan como base de seguridad mínima
  - Implementar medidas de seguridad adicionales, como la autenticación multifactor
  - Evitar tareas y acciones no estándar que realizan los roles no aprobados

Proceso

La asignación de control preventivo es el proceso de asignar controles a los requisitos y utilizar políticas para implementar esos controles mediante la restricción, la desactivación o el bloqueo. Al asignar los controles, tenga en cuenta el efecto proactivo que tienen en el entorno, los recursos y los usuarios. Las siguientes son prácticas recomendadas para la asignación de controles:

- Los controles estrictos que prohíben una actividad se deben asignar a los entornos de producción en los que la acción requiera procesos de revisión, aprobación y cambio.
- Los entornos de desarrollo o confinados pueden tener menos controles preventivos para ofrecer la agilidad que se necesita para crear y probar.
- La clasificación de datos, el nivel de riesgo de un activo y la política de administración de riesgos determinan los controles preventivos.
- Asigne los marcos existentes como prueba de la conformidad con los estándares y reglamentos.
- Implemente controles preventivos por ubicación geográfica, entorno, cuentas, redes, usuarios, roles o recursos.

Casos de uso

Gestión de datos

Se crea un rol que puede acceder a todos los datos de una cuenta. Si hay datos confidenciales y cifrados, los privilegios excesivamente permisivos pueden suponer un riesgo, en función de los usuarios o grupos que puedan asumir el rol. Al usar una política de claves en AWS Key Management Service (AWS KMS), puedes controlar quién tiene acceso a la clave y descifrar los datos.

Escalado de privilegios

Si los permisos administrativos y de escritura se asignan de una forma demasiado amplia, el usuario puede eludir los límites de los permisos previstos y concederse privilegios adicionales. El usuario que crea y administra un rol puede asignar un límite de permisos, que define los privilegios máximos permitidos para el rol.

Bloqueo de carga de trabajo

Si su empresa no tiene una necesidad previsible de utilizar servicios específicos, active una política de control de servicios que limite los servicios que pueden funcionar en las cuentas de los miembros

de una organización o restrinja los servicios en función de ellos. Región de AWS Este control preventivo puede reducir el alcance del impacto si un agente de amenazas logra comprometer una cuenta de su organización y acceder a ella. Para obtener más información, consulte la sección Políticas de control de servicios de esta guía.

Impacto en otras aplicaciones

Los controles preventivos pueden imponer el uso de servicios y características, como IAM, el cifrado y el registro, para cumplir con los requisitos de seguridad de las aplicaciones. También puede utilizar estos controles para protegerse contra las vulnerabilidades al limitar las acciones que un agente de amenazas puede aprovechar debido a errores involuntarios o a una mala configuración.

Tecnología

Políticas de control de servicios

En AWS Organizations, las políticas de control de servicios (SCP) definen los permisos máximos disponibles para las cuentas de los miembros de una organización. Estas políticas ayudan a las cuentas a cumplir con las directrices de control de acceso de la organización. Tenga en cuenta lo siguiente al diseñar las SCP para su organización:

- Los SCP son controles preventivos porque definen y hacen cumplir los permisos máximos permitidos para las funciones y los usuarios de IAM en las cuentas de los miembros de la organización.
- Los SCP afectan únicamente a los roles y usuarios de IAM en las cuentas de los miembros de la organización. No afectan a los usuarios ni a los roles de la cuenta de administración de la organización.

Puede hacer que una SCP sea más detallada al definir los permisos máximos para cada Región de AWS.

Límites de permisos de IAM

En AWS Identity and Access Management (IAM), se utiliza un límite de permisos para establecer el número máximo de permisos que una política basada en la identidad puede conceder a una entidad de IAM (usuarios o roles). Un límite de permisos para una entidad le posibilita realizar solo las acciones que le permitan tanto sus políticas basadas en identidades como sus límites de permisos. Tenga en cuenta lo siguiente al usar los límites de permisos:

- Puede utilizar una política gestionada o una política AWS gestionada por el cliente para establecer el límite de una entidad de IAM.
- Un límite de permisos no concede permisos por sí mismo. La política de límite de permisos limita los permisos que se conceden a la entidad de IAM.

Resultados empresariales

Ahorro de tiempo

- Al agregar la automatización después de configurar los controles preventivos, puede reducir la necesidad de intervención manual y reducir la frecuencia de los errores.
- El uso de los límites de permisos como control preventivo ayuda a los equipos de seguridad y de IAM a centrarse en tareas críticas, como la gobernanza y la asistencia.

Conformidad normativa

- Es posible que las empresas deban cumplir con las normas internas o industriales. Pueden ser restricciones regionales, de usuarios y roles o de servicio. Las SCP pueden ayudarlo a cumplir con las normas y evitar sanciones por infracción.

Reducción de riesgos

- Con el crecimiento, aumenta la cantidad de solicitudes para crear y administrar políticas y roles nuevos. Resulta cada vez más difícil comprender el contexto de lo que se requiere a fin de crear los permisos para cada aplicación de forma manual. El establecimiento de controles preventivos actúa como punto de partida y ayuda a evitar que los usuarios realicen acciones no deseadas, incluso si se les ha concedido el acceso de forma accidental.
- La aplicación de controles preventivos a las políticas de acceso brinda una capa adicional para ayudar a proteger los datos y activos.

Controles proactivos

Los controles proactivos son controles de seguridad que se diseñaron para evitar la creación de recursos que no cumplan con las normas. Estos controles pueden reducir la cantidad de eventos de seguridad que gestionan los controles de respuesta y de detección. Estos controles garantizan que

los recursos implementados cumplan con las normas antes de su implementación; por lo tanto, no hay ningún evento de detección que requiera una respuesta o una corrección.

Por ejemplo, puede contar con un control de detección que le notifique si un bucket de Amazon Simple Storage Service (Amazon S3) pasa a ser de acceso público. También es posible que tenga un control de respuesta que corrija esto. Si bien ya cuenta con estos dos controles, puede agregar otra capa de protección con un control proactivo. De este AWS CloudFormation modo, el control proactivo puede impedir la creación de actualizaciones en cualquier bucket de S3 que tenga habilitado el acceso público. Los actores de amenazas aún podrían eludir este control e implementar o modificar recursos fuera de él CloudFormation. En este caso, los controles de detección y de respuesta solucionarían el evento de seguridad.

Revise la siguiente información acerca de este tipo de controles:

- Objetivos
- Proceso
- Casos de uso
- Tecnología
- Resultados empresariales

Objetivos

- Los controles proactivos lo ayudan a mejorar las operaciones de seguridad y los procesos de calidad.
- Los controles proactivos pueden ayudarlo a cumplir con las políticas de seguridad, los estándares y las obligaciones normativas o de conformidad.
- Los controles proactivos pueden impedir la creación de recursos que no cumplan con las normas.
- Los controles proactivos pueden reducir la cantidad de resultados de seguridad.
- Los controles proactivos proporcionan otra capa de protección frente a los agentes de amenazas que eluden los controles preventivos e intentan implementar recursos que no cumplen con las normas.
- En combinación con los controles preventivos, de detección y de respuesta, los controles proactivos pueden ayudarlo a abordar posibles incidentes de seguridad.

Proceso

Los controles proactivos complementan a los controles preventivos. Los controles proactivos reducen el riesgo de seguridad de su organización y exigen la implementación de recursos que cumplan con las normas. Estos controles evalúan la conformidad de los recursos antes de crearlos o actualizarlos. Los controles proactivos generalmente se implementan mediante CloudFormation ganchos. Si el recurso no supera la validación de los controles proactivos, puede elegir entre generar un error de implementación del recurso o mostrar un mensaje de advertencia. A continuación se ofrecen algunos consejos y prácticas recomendadas para crear controles proactivos:

- Asegúrese de que los controles proactivos se adapten a los requisitos de conformidad de su organización.
- Asegúrese de que los controles proactivos sigan las prácticas recomendadas de seguridad del servicio asociado.
- Utilice CloudFormation StackSets u otra solución para implementar controles proactivos en varias cuentas Regiones de AWS OR.
- Asegúrese de que el mensaje de advertencia o error asociado a un control proactivo sea explícito y claro. Esto ayuda a los desarrolladores a entender el motivo por el que el recurso no superó la evaluación.
- Al crear nuevos controles proactivos, comience en el modo de observación. Esto significa que envía un mensaje de advertencia en lugar de generar un error en la implementación del recurso. Esto lo ayuda a comprender el impacto del control proactivo.
- Habilite el inicio de sesión en Amazon CloudWatch Logs para realizar controles proactivos.
- Si necesitas monitorear la invocación de un control proactivo específico, usa una EventBridge regla de Amazon y suscríbete a los eventos de invocación del CloudFormation gancho.

Casos de uso

- Impedir la implementación de recursos que no cumplan con las normas.
- Cumplir con los requisitos de conformidad.
- Exigir la corrección de un problema de seguridad antes de la implementación para mejorar la calidad del código.
- Reducir el tiempo de inactividad operativo asociado a la solución de los problemas de seguridad tras la implementación.

Tecnología

CloudFormation ganchos

AWS CloudFormationle ayuda a configurar AWS los recursos, aprovisionarlos de forma rápida y coherente y administrarlos a lo largo de su ciclo de vida en todas Cuentas de AWS las regiones. CloudFormation Hooks evalúa de forma proactiva la configuración de sus CloudFormation recursos antes de implementarlos. Si se encuentran recursos que no cumplen con las normas, devuelve un estado de error. En función del modo de fallo del gancho, CloudFormation pueden fallar en la operación o presentar una advertencia que permita al usuario continuar con la implementación. Puede usar los enlaces disponibles o puede desarrollar los suyos propios.

AWS Control Tower

AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas, siguiendo las mejores prácticas prescriptivas. AWS Control Tower ofrece controles proactivos preconfigurados que puedes activar en tu landing zone. Si tu landing zone está configurada mediante AWS Control Tower, puedes usar estos controles proactivos opcionales como punto de partida para tu organización. Puede incorporar controles proactivos adicionales y personalizados CloudFormation según sea necesario.

Resultados empresariales

Menos errores y esfuerzo humano

Los controles proactivos reducen el riesgo de errores humanos que provocan la implementación de recursos que no cumplen con las normas. También reducen el esfuerzo humano en las fases posteriores del ciclo de desarrollo, ya que hacen que los desarrolladores consideren la seguridad de los recursos antes de la implementación. Esto aplica la práctica de desplazamiento a la izquierda para crear recursos seguros, ya que exige la conformidad en las primeras fases del ciclo de vida del desarrollo.

Reducción de los costos

Por lo general, es más caro solucionar un problema de seguridad después de la implementación. Identificar y solucionar los problemas en las primeras fases del ciclo de desarrollo reduce el costo del desarrollo.

Ahorro de tiempo

Como los controles proactivos impiden la implementación de recursos que no cumplen con las normas, reducen la cantidad de tiempo que se dedica a clasificar y solucionar los problemas de seguridad. También reducen el número de resultados de seguridad, que los controles de detección identificarían en las fases posteriores del ciclo de desarrollo.

Conformidad normativa

Si su organización debe cumplir con las normativas internas o del sector, los controles proactivos pueden ayudarlo a cumplirlas y evitar sanciones por infracciones.

Reducción de riesgos

Los controles proactivos ayudan a los desarrolladores a implementar recursos creados de forma más segura y que cumplen con las normas, por lo que los controles proactivos reducen el riesgo de seguridad de su organización.

Controles de detección

Los controles de detección son controles de seguridad que se han diseñado para detectar, registrar y alertar después de que se produzca un evento. Los controles de detección son una parte fundamental de los marcos de gobernanza. Estas barreras de protección son una segunda línea de defensa, ya que le notifican los problemas de seguridad que han eludido los controles preventivos.

Por ejemplo, puede aplicar un control de detección para detectar y notificar si un bucket de Amazon Simple Storage Service (Amazon S3) pasa a ser de acceso público. Si bien es posible que disponga de controles preventivos que inhabiliten el acceso público a los buckets de S3 a nivel de cuenta y, posteriormente, inhabiliten el acceso a través de las SCP, un agente de amenazas puede eludir estos controles preventivos si inicia sesión como usuario administrativo. En estas situaciones, un control de detección puede alertarlo sobre los errores de configuración y la posible amenaza.

Revise la siguiente información acerca de este tipo de controles:

- Objetivos
- Proceso
- Casos de uso
- Tecnología
- Resultados empresariales

Objetivos

- Los controles de detección lo ayudan a mejorar los procesos de operaciones de seguridad y los procesos de calidad.
- Los controles de detección lo ayudan a cumplir con las obligaciones reglamentarias, legales o de conformidad.
- Los controles de detección ofrecen visibilidad a los equipos de operaciones de seguridad para responder a los problemas de seguridad, incluidas las amenazas avanzadas que eluden los controles preventivos.
- Los controles de detección pueden ayudarlo a identificar la respuesta adecuada a los problemas de seguridad y las posibles amenazas.

Proceso

Los controles de detección se implementan en dos fases. En primer lugar, debe configurar el sistema para registrar los eventos y los estados de los recursos en una ubicación centralizada, como Amazon CloudWatch Logs. Una vez que se establece el registro centralizado, estos se analizan para detectar anomalías que puedan indicar una amenaza. Cada análisis es un control que se asigna a sus requisitos y políticas originales. Por ejemplo, puede crear un control de detección que busque un patrón específico en los registros y genere una alerta si coincide. Los equipos de seguridad utilizan los controles de detección para mejorar su visibilidad general de las amenazas y los riesgos a los que su sistema podría estar expuesto.

Casos de uso

Detección de comportamiento sospechoso

Los controles de detección ayudan a identificar cualquier actividad anómala, como credenciales de usuarios privilegiados comprometidas o el acceso o la fuga de datos confidenciales. Estos controles son factores reactivos importantes que pueden ayudar a su empresa a identificar y comprender el alcance de la actividad anómala.

Detección de fraude

Estos controles ayudan a detectar e identificar una amenaza dentro de la empresa, como un usuario que elude las políticas y realiza transacciones no autorizadas.

Conformidad

Los controles de detección ayudan a cumplir los requisitos de conformidad, como las Normas de seguridad de datos del sector de las tarjetas de pago (PCI DSS), y pueden ayudar a prevenir el robo de identidad. Estos controles pueden ayudarlo a descubrir y proteger la información confidencial que se encuentra sujeta a la conformidad normativa, como la información de identificación personal.

Análisis automatizado

Los controles de detección pueden analizar de forma automática los registros para detectar anomalías y otros indicadores de actividad no autorizada.

Puede analizar de forma automática los registros de diferentes orígenes, como registros de AWS CloudTrail , Registro de flujo de la VPC y registros del sistema de nombres de dominio (DNS) para indicar una actividad potencialmente maliciosa. Para facilitar la organización, agrupe las alertas de seguridad o los hallazgos de varias Servicios de AWS ubicaciones en una ubicación centralizada.

Tecnología

Un control de detección habitual consiste en implementar uno o más servicios de monitoreo, que pueden analizar los orígenes de datos, como los registros, para identificar las amenazas de seguridad. En el Nube de AWS, puede analizar fuentes como AWS CloudTrail los registros, los registros de acceso a Amazon S3 y los registros de flujo de Amazon Virtual Private Cloud para ayudar a detectar actividades inusuales. AWS los servicios de seguridad, como Amazon GuardDuty, Amazon Detective y Amazon Macie AWS Security Hub, tienen funcionalidades de monitoreo integradas.

GuardDuty y Security Hub

Amazon GuardDuty utiliza técnicas de inteligencia de amenazas, aprendizaje automático y detección de anomalías para supervisar continuamente las fuentes de registro en busca de actividades maliciosas o no autorizadas. El panel de control proporciona información sobre su estado Cuentas de AWS y el de sus cargas de trabajo en tiempo real. Puede integrarlo GuardDuty con AWS Security Hubun servicio de gestión del estado de seguridad en la nube que comprueba el cumplimiento de las mejores prácticas, agrega alertas y permite la corrección automática. GuardDuty envía los resultados a Security Hub como una forma de centralizar la información. Puede integrar aún más Security Hub con las soluciones de administración de eventos e información de seguridad (SIEM) para ampliar las capacidades de monitoreo y alerta de su organización.

Macie

Amazon Macie es un servicio de privacidad y seguridad de datos completamente administrado que utiliza machine learning y coincidencia de patrones para ayudar a descubrir y proteger los datos confidenciales en AWS. Las siguientes son algunas de las características y controles de detección disponibles en Macie:

- Macie inspecciona el inventario de bucket y todos los objetos almacenados en Amazon S3. Esta información se puede presentar en una única vista de panel, lo que brinda visibilidad y lo ayuda a evaluar la seguridad de los buckets.
- Para descubrir datos confidenciales, Macie utiliza identificadores de datos administrados e integrados y también admite identificadores de datos personalizados.
- Macie se integra de forma nativa con otras Servicios de AWS herramientas. Por ejemplo, Macie publica las conclusiones como EventBridge eventos de Amazon, que se envían automáticamente a Security Hub.

Las siguientes son prácticas recomendadas para configurar los controles de detección en Macie:

- Habilite Macie en todas las cuentas. Al utilizar la característica de administración delegada, habilite a Macie en varias cuentas mediante AWS Organizations.
- Utilice Macie para evaluar la posición de seguridad de los buckets de S3 de sus cuentas. Esto ayuda a evitar la pérdida de datos y brinda visibilidad de la ubicación y el acceso a los datos. Para obtener más información, consulte Análisis de su posición de seguridad de Amazon S3 (documentación de Macie).
- Automatice la detección de datos confidenciales en sus buckets de S3 al ejecutar y programar tareas automatizadas de procesamiento y descubrimiento de datos. Esto inspecciona los buckets de S3 en busca de datos confidenciales de forma periódica.

AWS Config

AWS Configaudita y registra el cumplimiento de los AWS recursos. AWS Config descubre AWS los recursos existentes y genera un inventario completo, junto con los detalles de configuración de cada recurso. Si hay algún cambio en la configuración, registra esos cambios y envía una notificación. Esto puede ayudarlo a detectar y revertir los cambios de infraestructura no autorizados. Puede usar reglas AWS administradas y puede crear reglas personalizadas.

Las siguientes son prácticas recomendadas para configurar los controles de detección en AWS Config:

- AWS Config Actívela para cada cuenta de miembro de la organización y para cada una de las cuentas Región de AWS que contengan los recursos que desee proteger.
- Configure las alertas de Amazon Simple Notification Service (Amazon SNS) para cualquier cambio de configuración.
- Guarde los datos de configuración en un bucket de S3 y utilice Amazon Athena para analizarlos.
- Automatice la corrección de los recursos no conformes mediante el uso de la Automatización, una capacidad de AWS Systems Manager.
- Utilice EventBridge Amazon SNS para configurar notificaciones sobre recursos no AWS conformes.

Trusted Advisor

Se puede utilizar AWS Trusted Advisor como un servicio para los controles de detección. Mediante un conjunto de comprobaciones, Trusted Advisor identifica las áreas en las que puede optimizar su infraestructura, mejorar el rendimiento y la seguridad o reducir los costos. Trusted Advisor proporciona recomendaciones basadas en las AWS mejores prácticas que puede seguir para mejorar sus servicios y recursos. Los planes Business y Enterprise Support proporcionan acceso a todas las comprobaciones disponibles para los pilares del AWS Well-Architected Framework.

Las siguientes son prácticas recomendadas para configurar los controles de detección en Trusted Advisor:

- Analice el resumen del nivel de comprobación.
- Implemente recomendaciones específicas de recursos para los estados de advertencia y error.
- Trusted Advisor Compruébelo con frecuencia para revisar e implementar activamente sus recomendaciones.

Amazon Inspector

Amazon Inspector es un servicio automatizado de administración de vulnerabilidades que, después de habilitarse, analiza de forma continua las cargas de trabajo en busca de cualquier exposición de la red no deseada o vulnerabilidades de software. Contextualiza los resultados en una puntuación de

riesgo que puede ayudarlo a determinar los próximos pasos, como corregir o confirmar el estado de conformidad.

Las siguientes son prácticas recomendadas para configurar los controles de detección en Amazon Inspector:

- Active Amazon Inspector en todas las cuentas e intégrelo en EventBridge un Security Hub para configurar los informes y las notificaciones de las vulnerabilidades de seguridad.
- Priorice las correcciones y otras medidas en función de la puntuación de riesgo de Amazon Inspector.

Resultados empresariales

Menos errores y esfuerzo humano

Puede lograr la automatización mediante el uso de la infraestructura como código (IaC). La automatización de la implementación y la configuración de los servicios y herramientas de monitoreo y corrección reduce el riesgo de errores manuales y la cantidad de tiempo y esfuerzo necesarios para escalar estos controles de detección. La automatización ayuda a desarrollar manuales de procedimientos de seguridad y reduce las operaciones manuales para los analistas de seguridad. Las revisiones periódicas ayudan a ajustar las herramientas de automatización y a iterar y mejorar los controles de detección de forma continua.

Medidas adecuadas contra las posibles amenazas

Registrar y analizar los eventos a partir de registros y métricas es fundamental para ganar visibilidad. Esto ayuda a los analistas a actuar ante los eventos de seguridad y las posibles amenazas para proteger las cargas de trabajo. La capacidad de identificar las vulnerabilidades que existen con rapidez ayuda a los analistas a tomar las medidas adecuadas para abordarlas y solucionarlas.

Mejor respuesta a incidentes y gestión de la investigación

La automatización de las herramientas de control de detección puede aumentar la velocidad de detección, investigación y recuperación. Las alertas y notificaciones automatizadas basadas en condiciones definidas permiten a los analistas de seguridad investigar y responder de manera adecuada. Estos factores de respuesta pueden ayudarlo a identificar y comprender el alcance de la actividad anómala.

Controles de respuesta

Los controles de respuesta son controles de seguridad que se han diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Algunos ejemplos de controles de respuesta técnica incluyen la aplicación de revisiones a un sistema, el aislamiento de un virus, el cierre de un proceso o el reinicio de un sistema.

Revise la siguiente información acerca de este tipo de controles:

- Objetivos
- Proceso
- Casos de uso
- Tecnología
- Resultados empresariales

Objetivos

- Los controles de respuesta pueden ayudarlo a crear manuales de procedimientos para los tipos de ataques más comunes, como la suplantación de identidad o los ataques de fuerza bruta.
- Los controles de respuesta pueden implementar respuestas automatizadas a posibles problemas de seguridad.
- Los controles responsivos pueden corregir automáticamente las acciones no deseadas o no aprobadas en relación con AWS los recursos, como la eliminación de depósitos de S3 no cifrados.
- Los controles de respuesta se pueden orquestar para que funcionen con controles preventivos y de detección, a fin de crear un enfoque integral y proactivo para abordar los posibles incidentes de seguridad.

Proceso

Los controles de detección son un requisito previo para establecer controles de respuesta. Debe poder detectar el problema de seguridad antes de poder solucionarlo. Luego, puede establecer una política o una respuesta al problema de seguridad. Por ejemplo, en caso de un ataque de fuerza bruta, se implementaría un proceso de corrección. Una vez que finalice el proceso de corrección, se puede automatizar y ejecutar como un script mediante un lenguaje de programación, como un script del intérprete de comandos.

Considere si el control de respuesta podría interrumpir una carga de trabajo de producción existente. Por ejemplo, si el control de seguridad de detección es Los buckets de S3 no deben ser de acceso público y la corrección es desactivar el acceso público a Amazon S3, esto podría tener consecuencias importantes para su empresa y sus clientes. Si el bucket de S3 brinda servicio a un sitio web público, desactivar el acceso público podría provocar una interrupción. Las bases de datos son un ejemplo similar. Si una base de datos no debe ser de acceso público a través de Internet, desactivar el acceso público podría afectar a la conectividad con la aplicación.

Casos de uso

- Respuesta automática a los eventos de seguridad detectados
- Corrección automática de las vulnerabilidades de seguridad detectadas
- Control de recuperación automatizado para reducir el tiempo de inactividad operativo

Tecnología

Security Hub

AWS Security Hubenvía automáticamente todos los hallazgos nuevos y todas las actualizaciones de los hallazgos existentes como eventos. EventBridge También puede crear acciones personalizadas a las que se envíen los hallazgos seleccionados y los resultados de información EventBridge. Puede configurarlo EventBridge para responder a cada tipo de evento. El evento puede iniciar una AWS Lambda función que lleve a cabo la acción correctiva.

AWS Config

AWS Configutiliza reglas para evaluar sus AWS recursos y le ayuda a corregir los recursos que no cumplen con las normas. AWS Config aplica la remediación mediante la automatización.AWS Systems Manager En los documentos de automatización, usted define las acciones que desea realizar en los recursos que se AWS Config determine que no cumplen con los requisitos. Después de crear los documentos de automatización, puede utilizarlos en Systems Manager a través de las API AWS Management Console o mediante ellas. Puede elegir corregir de forma manual o automática los recursos no conformes.

Resultados empresariales

Minimizar la pérdida de datos

Tras un incidente de ciberseguridad, el uso de controles de seguridad de respuesta puede ayudar a minimizar la pérdida de datos y los daños al sistema o la red. Los controles de respuesta también pueden ayudar a restaurar los sistemas y procesos empresariales importantes lo más rápido posible, lo que aumenta la resistencia de las cargas de trabajo.

Reducir los costos

La automatización reduce los costes asociados a los recursos humanos, ya que los miembros del equipo no tienen que responder manualmente a los incidentes ni gestionarlos de case-by-case forma independiente.

Siguientes pasos

Tras leer esta guía, debería estar familiarizado con los cuatro tipos de controles de seguridad, comprender de qué manera forman parte de su marco de gobernanza de seguridad y estar preparado para comenzar a implementar y automatizar los controles de seguridad en la Nube de AWS. Para obtener más información, recomendamos que repase las referencias que se incluyen en la sección Recursos.

También le recomendamos que siga los pasos siguientes para evaluar la seguridad de su infraestructura en la nube y comenzar a implementar controles de seguridad:

1. Habilite y configure AWS Security Hub. Como práctica recomendada, sugerimos habilitar los controles de estándares disponibles. Para obtener más información, consulte Estándares y controles de seguridad (documentación de Security Hub).
2. Habilite y configure AWS Config. Para obtener más información, consulte Introducción (documentación de AWS Config).
3. Mediante Servicios de AWS como Security Hub, Amazon Macie, AWS Config, AWS Trusted Advisor y Amazon Inspector, evalúe la infraestructura de su organización y su cuenta, identifique las áreas que necesitan mejoras y analice y recomiende estos servicios. Utilice la característica de control de seguridad de Security Hub a fin de generar una puntuación de seguridad para un estándar de seguridad. Para obtener más información, consulte Determining security scores (documentación de Security Hub).
4. Implemente controles de seguridad preventivos, proactivos, de detección y de respuesta en función de las mejoras identificadas.
5. Realice una evaluación de seguridad de seguimiento para evaluar la eficacia de los controles de seguridad implementados. En Security Hub, determine si la puntuación de seguridad ha mejorado. Realice iteraciones para mejorar o agregar controles de seguridad nuevos.
6. Establezca una frecuencia regular para realizar las evaluaciones de seguridad, por ejemplo, una vez al año.

Preguntas frecuentes

¿En qué debo enfocarme si tengo tiempo y recursos limitados y no puedo implementar todos estos tipos de controles?

Recomendamos implementar AWS Security Hub. Security Hub cuenta con un conjunto de controles de seguridad automatizados denominado Estándar de Prácticas recomendadas de seguridad básica de AWS (documentación de Security Hub). Se trata de un conjunto seleccionado de prácticas recomendadas de seguridad que administran expertos en seguridad de AWS. Puede ejecutar estos controles estándar de forma continua, siempre que se produzcan cambios en los recursos asociados, o de manera periódica, siguiendo un programa regular. Cada control cuenta con una puntuación de gravedad específica para ayudarlo a priorizar sus esfuerzos de remediación. Para obtener más información, consulte Ejecución de controles de seguridad (documentación de Security Hub). Si utiliza AWS Control Tower, también puede revisar y habilitar sus controles preventivos, de detección y proactivos.

Recursos

Documentación de AWS

- Arquitectura de referencia de seguridad de AWS (SRA de AWS)
- AWS CAF security perspective
- Prácticas recomendadas para seguridad, identidad y conformidad
- Respuesta de seguridad automatizada en AWS (Solución de AWS)
  - Página de inicio de la solución
  - Guía de implementación

Publicaciones de blog de AWS

- Guía de Identity: controles preventivos con AWS Identity, SCP
- Cómo implementar una política de control de servicio (SCP) de solo lectura para las cuentas en AWS Organizations
- Prácticas recomendadas para las políticas de control de servicio de AWS Organizations en un entorno de varias cuentas
- Mantener la conformidad mediante las políticas de control de servicio y asegurarse de que se apliquen siempre
- Cuándo y dónde utilizar los límites de permisos de IAM
- Proactively keep resources secure and compliant with AWS CloudFormation hooks

Otros recursos

- Matriz de controles en la nube (CCM) (Cloud Security Alliance)
- Límites de permisos de ejemplo (GitHub)

Historial del documento

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
Controles proactivos	Agregamos información sobre los controles proactivos a esta guía, incluida la sección Controles proactivos.	4 de diciembre de 2023
Publicación inicial	—	12 de diciembre de 2022

AWS Glosario de orientación prescriptiva

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

Números

Las 7 R

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

- Refactorizar/rediseñar: traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: migre su base de datos Oracle local a la edición compatible con 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 instancia EC2 del. Nube de AWS
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma local a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

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

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

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

migración activa-pasiva

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

función agregada

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 se utiliza AIOps en la estrategia de migración de AWS , 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

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

botnet

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

rama

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

acceso con cristales rotos

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

estrategia de implementación sobre infraestructura existente

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

caché de búfer

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

capacidad empresarial

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

planificación de la continuidad del negocio (BCP)

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

C

CAF

Consulte el marco AWS de adopción de la nube.

despliegue canario

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

CCoE

Consulte el Centro de excelencia en la nube.

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 CCoE 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: realización de inversiones fundamentales para escalar la adopción de la nube (p. ej., crear una zona de aterrizaje, definir un CCoE, 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 del blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la guía de preparación para la migración.

CMDB

Consulte la base de datos de administración de la configuración.

repositorio de código

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

caché en frío

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

datos fríos

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

visión artificial (CV)

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

desviación de configuración

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

base de datos de administración de configuración (CMDB)

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, 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, presentación y producción del proceso de lanzamiento del software. La CI/CD se describe comúnmente como una canalización. La CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Consulte visión artificial.

D

datos en reposo

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

clasificación de datos

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

desviación de datos

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

datos en tránsito

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

malla de datos

Un marco arquitectónico que proporciona una propiedad de datos distribuida y descentralizada con 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 desviaciones

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

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

computación en la periferia

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

cifrado

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

clave de cifrado

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

endianidad

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

punto de conexión

Consulte el punto final del servicio.

servicio de punto de conexión

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).

environment

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

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

epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, las 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.

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.

G

bloqueo geográfico

Consulta las restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

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

Flujo de trabajo de Gitflow

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

estrategia de implementación desde cero

La ausencia de infraestructura existente en un entorno nuevo. Al adoptar una estrategia de implementación desde cero para una arquitectura de sistemas, puede seleccionar todas las tecnologías nuevas sin que estas deban ser compatibles con una infraestructura existente, lo que también se conoce como implementación sobre infraestructura existente. Si está ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y la conformidad en todas las unidades organizativas (OU). 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

JA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

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

alta disponibilidad (HA)

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

modernización histórica

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

migración homogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que comparte el mismo motor de base de datos (por ejemplo, Microsoft SQL Server a Amazon RDS 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 DevOps versiones.

periodo de hiperatención

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

I

IaC

Vea la infraestructura como código.

políticas basadas en identidad

Política asociada a uno o más 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, aplicar parches o modificar la infraestructura existente. Las infraestructuras inmutables son intrínsecamente más consistentes, fiables y predecibles que las infraestructuras mutables. Para obtener más información, consulte las prácticas recomendadas para implementar con una infraestructura inmutable en Well-Architected Framework AWS .

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 de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

migración gradual

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

Industria 4.0

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

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial (IIoT)

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

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red entre las VPC (iguales o Regiones de AWS diferentes), Internet y las redes locales. La Arquitectura de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su 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 más información, consulte Interpretabilidad del modelo de machine learning 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.

migración grande

Migración de 300 servidores o más.

LBAC

Consulte el control de acceso basado en etiquetas.

privilegio mínimo

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

migrar mediante lift-and-shift

Ver 7 Rs.

sistema little-endian

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

entornos inferiores

Véase entorno.

M

machine learning (ML)

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

rama principal

Ver sucursal.

malware

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

servicios gestionados

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

sistema de ejecución de fabricación (MES)

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

MAP

Consulte Migration Acceleration Program.

mecanismo

Un proceso completo en el que se crea una herramienta, se impulsa su adopción y, a continuación, se inspeccionan los resultados para realizar 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 API bien definidas 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 servicios sin servidor. AWS

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 API ligeras. 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: rehospede la migración a Amazon EC2 AWS con Application Migration Service.

Migration Portfolio Assessment (MPA)

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

tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de oleadas). La herramienta MPA (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores asociados de APN.

Evaluación de la preparación para la migración (MRA)

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

estrategia de migración

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

ML

Consulte el aprendizaje automático.

modernización

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

evaluación de la preparación para la modernización

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

aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la

aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar una arquitectura de microservicios. Para obtener más información, consulte Descomposición de monolitos en microservicios.

MAPA

Consulte la evaluación de la cartera de migración.

MQTT

Consulte Message Queue Queue Telemetría y Transporte.

clasificación multiclase

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

infraestructura mutable

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

O

OAC

Consulte el control de acceso de origen.

OAI

Consulte la identidad de acceso de origen.

OCM

Consulte gestión del cambio organizacional.

migración fuera de línea

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

OI

Consulte integración de operaciones.

OLA

Véase el acuerdo a nivel operativo.

migración en línea

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

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

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

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

acuerdo de nivel operativo (OLA)

Acuerdo que aclara lo que los grupos de TI operativos se comprometen a ofrecerse entre sí, para respaldar un acuerdo de nivel de servicio (SLA).

revisión de la preparación operativa (ORR)

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

tecnología operativa (OT)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En la industria manufacturera, la integración de los sistemas de TO y tecnología de la información (TI) es un enfoque clave para las transformaciones de la industria 4.0.

integración de operaciones (OI)

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

registro de seguimiento organizativo

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

administración del cambio organizacional (OCM)

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

control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso y proteger el contenido del Amazon Simple Storage Service (Amazon S3). El OAC admite todos los buckets de S3 Regiones de AWS, el cifrado del lado del servidor AWS KMS (SSE-KMS) y las solicitudes dinámicas `PUT` y `DELETE` dirigidas al bucket de S3.

identidad de acceso de origen (OAI)

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

O

Consulte la revisión de la preparación operativa.

NO

Consulte 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 de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su 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.

política

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

persistencia políglota

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

evaluación de cartera

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

predicate

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

pulsar un predicado

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

control preventivo

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

entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz 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 ingeniería.

zonas alojadas privadas

Contenedor que aloja información acerca de cómo desea que responda Amazon Route 53 a las consultas de DNS de un dominio y sus subdominios en una o varias VPC. 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.

seudonimización

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

publicar/suscribirse (pub/sub)

Un patrón que permite las comunicaciones asíncronas entre microservicios para mejorar la escalabilidad y la capacidad de respuesta. Por ejemplo, en un 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).

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.

read replica

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

rediseñar

Ver 7 Rs.

objetivo de punto de recuperación (RPO)

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

objetivo de tiempo de recuperación (RTO)

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

refactorizar

Ver 7 Rs.

Región

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

regresión

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

volver a alojar

Consulte 7 Rs.

versión

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

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

resilencia

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

política basada en recursos

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

matriz responsable, 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.

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.

control de seguridad

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

refuerzo de la seguridad

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

sistema de información 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 instancia de Amazon EC2 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)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. Las SCP definen barreras de protección o establecen límites a las acciones que un administrador puede delegar en los usuarios o roles. Puede utilizar las SCP como listas de permitidos o rechazados, para especificar qué servicios o acciones se encuentra 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.

ASÍ QUE

Consulte el objetivo de nivel de servicio.

split-and-seed modelo

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

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.

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

Centro de tránsito de red que puede utilizar para interconectar las VPC y las redes en las instalaciones. 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

Conexión entre dos VPC que 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 de calificación de cargas de trabajo de AWS.

escribe una vez, lee muchas (WORM)

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

Z

ataque de día cero

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

vulnerabilidad de día cero

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

aplicación zombi

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.