AWS Base de seguridad inicial (AWS SSB)

AWS Guía prescriptiva

AWS Guía prescriptiva: AWS Base de seguridad inicial (AWS SSB)

Table of Contents

Base de seguridad para startups de AWS (SSB de AWS)

Jay Michael de Amazon Web Services (AWS)

mayo de 2023 (historial de documentos)

La Base de seguridad para startups (SSB) de AWS es un conjunto de controles que crean una base mínima sobre la que las empresas pueden crear de forma segura en AWS sin disminuir su agilidad. Estos controles generan la base de su posición de seguridad y se centran en proteger las credenciales, permitir el registro y la visibilidad, administrar la información de contacto e implementar límites de datos básicos.

Los controles de esta guía se han diseñado pensando en las startups, a fin de mitigar los riesgos de seguridad más comunes sin requerir un esfuerzo significativo. Muchas startups comienzan su recorrido en la Nube de AWS con una sola Cuenta de AWS. A medida que las organizaciones crecen, migran a arquitecturas de varias cuentas. Las instrucciones de esta guía se han diseñado para arquitecturas de una sola cuenta, pero lo ayudan a configurar controles de seguridad que se migran o modifican con facilidad a medida que se realiza la transición a una arquitectura de varias cuentas.

Los controles de AWS SSB se dividen en dos categorías: cuenta y carga de trabajo. Los controles de cuenta ayudan a mantener su cuenta de AWS segura. Incluye recomendaciones para configurar el acceso de los usuarios, las políticas y los permisos, así como recomendaciones sobre cómo monitorear su cuenta a fin de detectar actividades no autorizadas o potencialmente maliciosas. Los controles de carga de trabajo ayudan a proteger los recursos y el código en la nube, como las aplicaciones, los procesos de backend y los datos. Incluye recomendaciones como el cifrado y la reducción del alcance del acceso.

> **Note**
>
> Algunos de los controles recomendados en esta guía sustituyen a los valores predeterminados que se establecieron durante la configuración inicial, mientras que la mayoría configura políticas y ajustes nuevos. Este documento no debe considerarse exhaustivo de todos los controles disponibles de ninguna manera.

Destinatarios previstos

Esta guía es la más adecuada para startups que se encuentran en las etapas iniciales de desarrollo, con un mínimo de personal y operaciones.

Las startups u otras empresas que se encuentran en etapas posteriores de operación y crecimiento aún pueden obtener un valor significativo al analizar estos controles en comparación con sus prácticas actuales. Si identifica alguna deficiencia, puede implementar los controles individuales de esta guía y luego evaluarlos para determinar su idoneidad como solución a largo plazo.

> **Note**
>
> Los controles que se recomiendan en esta guía son sobre aspectos fundamentales. Las startups u otras empresas que operen en una etapa posterior de escalado o sofisticación deberían agregar controles adicionales, según corresponda.

Marco de aspectos fundamentales y responsabilidades de seguridad

AWS Well-Architected ayuda a los arquitectos en la nube a crear infraestructuras seguras, de alto rendimiento, resistentes y eficientes para sus aplicaciones y cargas de trabajo. La Base de seguridad para startups de AWS se alinea con el pilar de seguridad del Marco de AWS Well-Architected. En el pilar de seguridad, se describe cómo aprovechar las tecnologías en la nube para proteger los datos, los sistemas y los activos de una manera que pueda mejorar su posición de seguridad. Esto lo ayuda a cumplir sus requisitos empresariales y reglamentarios siguiendo las recomendaciones actuales de AWS.

Puede evaluar su adhesión a las prácticas recomendadas de Well-Architected mediante AWS Well-Architected Tool en su cuenta de AWS.

La seguridad y conformidad son una responsabilidad compartida entre AWS y el cliente. El modelo de responsabilidad compartida se suele describir así: AWS es responsable de la seguridad en la nube (es decir, la protección de la infraestructura que ejecuta todos los servicios que se ofrecen en la Nube de AWS) y usted es responsable de la seguridad en la nube (según lo determinen los servicios de la Nube de AWS que seleccione). En el modelo de responsabilidad compartida, la implementación de los controles de seguridad de este documento forma parte de su responsabilidad como cliente.

Protección de la cuenta

Los controles y las recomendaciones de esta sección ayudan a mantener tu AWS cuenta segura. Hace hincapié en el uso de usuarios AWS Identity and Access Management (IAM), grupos de usuarios y funciones (también conocidos como principales) tanto para el acceso humano como por máquina, restringiendo el uso del usuario root y exigiendo la autenticación multifactor. En esta sección, confirmas que AWS tiene la información de contacto necesaria para comunicarte contigo en relación con la actividad y el estado de tu cuenta. También configuras servicios de monitoreo, como Amazon AWS Trusted Advisor, y GuardDuty AWS Budgets, para que se te notifique la actividad en tu cuenta y puedas responder rápidamente si la actividad no está autorizada o es inesperada.

Esta sección contiene los siguientes temas:

ACCT.01: establecer los contactos a nivel de cuenta en listas de distribución de correo electrónico válidas

Al configurar los contactos principales y alternativos para tu AWS cuenta, utiliza una lista de distribución de correo electrónico en lugar de la dirección de correo electrónico de una persona. El uso de una lista de distribución de correo electrónico garantiza que se preserven la propiedad y la

accesibilidad a medida que las personas de su organización entran y salen. Configura contactos alternativos para las notificaciones de facturación, operaciones y seguridad, y utiliza las listas de distribución de correo electrónico adecuadas en consecuencia. AWS utiliza estas direcciones de correo electrónico para ponerse en contacto con usted, por lo que es importante que mantenga el acceso a ellas.

Para editar el nombre de la cuenta, la contraseña del usuario raíz de o la dirección de correo electrónico del usuario raíz de

1. Inicie sesión en la página de Configuración de la cuenta en la consola de Administración de facturación y costos en https://console.aws.amazon.com/billing/home?#/account.
2. En la página Account Settings, junto a Account Settings, elija Edit.
3. Junto al campo que desea actualizar, elija Editar.
4. Una vez introducidos los cambios, elija Save changes.
5. Después de realizar todos los cambios, elija Done (Hecho).

Para editar la información de contacto

1. En la página de Configuración de la cuenta, en Información de contacto, elija Editar.
2. En el caso de los campos que desea cambiar, escriba la información actualizada y, a continuación, elija Actualizar.

Para agregar, actualizar o eliminar contactos alternativos

1. En la página de Configuración de la cuenta, en Contactos alternativos, elija Editar.
2. En el caso de los campos que desea cambiar, escriba la información actualizada y, a continuación, elija Actualizar.

ACCT.02: restringir el uso del usuario raíz

El usuario raíz se crea al abrir una AWS cuenta, y este usuario tiene todos los privilegios y permisos de propiedad sobre la cuenta que no se pueden cambiar. Utilizar el usuario raíz solo para las tareas específicas que lo requieran. Para obtener más información, consulte Tareas que requieren credenciales de usuario raíz (AWS Account Management). Realice todas las demás acciones en su cuenta mediante otros tipos de identidades de IAM, como usuarios federados con roles de IAM. Para obtener más información, consulte Credenciales de seguridad de AWS (documentación de IAM).

Para restringir el uso del usuario raíz

1. Requiere la autenticación multifactor (MFA) para el usuario raíz, como se describe en ACCT.05: requerir la autenticación multifactor (MFA) para iniciar sesión.
2. Cree un usuario administrativo para que no utilice el usuario raíz en las tareas cotidianas. Para obtener más información sobre la configuración del acceso de los usuarios, consulte ACCT.03: configurar el acceso a la consola para cada usuario.

ACCT.03: configurar el acceso a la consola para cada usuario

Como práctica recomendada, se AWS recomienda utilizar credenciales temporales para conceder acceso a los recursos Cuentas de AWS y a ellos. Las credenciales temporales tienen un ciclo de vida limitado, por lo que no tiene que rotarlas ni revocarlas de forma explícita cuando ya no las necesite. Para obtener más información, consulte Credenciales de seguridad temporales (documentación de IAM).

Para los usuarios humanos, se AWS recomienda utilizar identidades federadas de un proveedor de identidades (IdP) centralizado, AWS IAM Identity Center como Okta, Active Directory o Ping Identity. La federación de usuarios permite definir las identidades en una única ubicación central, y los usuarios pueden autenticarse de forma segura en varias aplicaciones y sitios web AWS, incluso mediante el uso de un solo conjunto de credenciales. Para obtener más información, consulte la federación de identidades en el AWS Centro de identidades de IAM (AWS sitio web).

> **Note**
>
> La federación de identidades puede complicar la transición de una arquitectura de una sola cuenta a una arquitectura de varias cuentas. Es habitual que las startups retrasen la implementación de la federación de identidades hasta que hayan establecido una arquitectura de varias cuentas administrada en AWS Organizations.

Para configurar la identidad federada

1. Si utiliza IAM Identity Center, consulte Introducción (documentación de IAM Identity Center).

   Si utiliza un IdP externo o de terceros, consulte Creación de proveedores de identidad de IAM (documentación de IAM).
2. Asegúrese de que su IdP aplique la autenticación multifactor (MFA).

3. Implemente los permisos en función de ACCT.04: asignar permisos.

En el caso de las startups que no se encuentran preparadas para configurar la federación de identidades, puede crear usuarios directamente en IAM. Esta no es una práctica recomendada de seguridad porque se trata de credenciales de larga duración que nunca caducan. Sin embargo, es una práctica habitual para las startups que están empezando a operar, a fin de evitar las dificultades que supone la transición a una arquitectura de una sola cuenta cuando se encuentran preparadas para operar.

Como punto de partida, puede crear un usuario de IAM para cada persona que necesite acceder a la AWS Management Console. Si configura los usuarios de IAM, no comparta las credenciales entre los usuarios y cambie las credenciales de larga duración de forma periódica.

> **Warning**
>
> Los usuarios de IAM tienen credenciales de larga duración, lo que supone un riesgo para la seguridad. Para ayudar a mitigar este riesgo, le recomendamos que brinde a estos usuarios únicamente los permisos que necesitan para realizar la tarea y que los elimine cuando ya no los necesiten.

Para crear un usuario de IAM

1. Crear usuarios de IAM (documentación de IAM).
2. Implemente los permisos en función de ACCT.04: asignar permisos.

ACCT.04: asignar permisos

Configure los permisos de usuario en la cuenta al asignar políticas a su identidad de IAM (rol o grupo de usuarios). Puede personalizar los permisos o adjuntar políticas AWS administradas, que son políticas independientes diseñadas AWS para proporcionar permisos en muchos casos de uso comunes. Si personaliza los permisos, siga las prácticas recomendadas de seguridad de conceder privilegios mínimos. El privilegio mínimo es la práctica de conceder el conjunto mínimo de permisos que cada usuario necesita para realizar sus tareas.

Si utiliza identidades federadas, los usuarios acceden a la cuenta al asumir un rol de IAM a través del proveedor de identidades externo. La función de IAM define lo que pueden hacer los usuarios

autenticados por el IdP de su organización. AWS Debe aplicar políticas personalizadas o AWS administradas a este rol para configurar los permisos.

Para asignar permisos a las identidades federadas

- Si utiliza IAM Identity Center, consulte Utilizar las políticas de IAM en los conjuntos de permisos (documentación de IAM Identity Center).

  Si utiliza un IdP externo o de terceros, consulte Adición de permisos de identidad de IAM (documentación de IAM).

Si utiliza usuarios de IAM, puede utilizar grupos de usuarios o roles para administrar los permisos de varios usuarios de IAM. Recomendamos los grupos de usuarios para las startups porque son más fáciles de administrar y son menos propensos a errores de configuración, lo que podría suponer un riesgo para la seguridad de su cuenta. Asigne los usuarios a los grupos de usuarios conforme a sus funciones laborales. Algunos ejemplos de grupos de usuarios son los ingenieros de aplicaciones, datos, redes y operaciones de desarrollo (DevOps). También puede dividir los tipos de usuarios en grupos de usuarios más pequeños en función de la autoridad que toma las decisiones, por ejemplo, para ingenieros con o sin experiencia.

Para asignar los permisos de los usuarios de IAM

1. Crear grupos de usuarios de IAM (documentación de IAM).
2. Adjunte una política AWS gestionada a un grupo de usuarios de IAM (documentación de IAM).

ACCT.05: requerir la autenticación multifactor (MFA) para iniciar sesión

Con MFA, los usuarios tienen un dispositivo que genera una respuesta a un reto de autenticación. Las credenciales de cada usuario y la respuesta generada por el dispositivo son necesarias para completar el proceso de inicio de sesión. Como práctica recomendada de seguridad, habilite la MFA para el Cuenta de AWS acceso, especialmente para las credenciales a largo plazo, como el usuario raíz de la cuenta y los usuarios de IAM.

Para configurar la MFA del usuario raíz

1. Inicie sesión en. AWS Management Console https://console.aws.amazon.com/

2. En la parte derecha de la barra de navegación, elija su nombre de cuenta y, a continuación, seleccione Mis credenciales de seguridad.
3. Si es necesario, elija Continue to Security Credentials (Continuar a credenciales de seguridad).
4. Amplíe la sección Multi-Factor Authentication (MFA) (Autenticación multifactor [MFA]) .
5. Elija Activate MFA (Activar MFA).
6. Siga las instrucciones del asistente para configurar los dispositivos con MFA en consecuencia. Para obtener más información, consulte Habilitación de los dispositivos con MFA para los usuarios en AWS (documentación de IAM).

Para configurar la MFA en IAM Identity Center

- Habilitar la MFA (documentación de IAM Identity Center)

Para configurar la MFA de su propio usuario de IAM

1. Con sus credenciales de inicio de sesión, inicie sesión en la consola de IAM en la https://console.aws.amazon.com/iam.
2. En la esquina superior derecha de la barra de navegación, elija su nombre de usuario y, a continuación, elija My Security Credentials (Mis credenciales de seguridad).
3. En la pestaña Credenciales de IAM AWS , en la sección Autenticación multifactor, elija Administrar dispositivos MFA.

Para configurar la MFA de otros usuarios de IAM

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala enhttps://console.aws.amazon.com/iam.
2. En el panel de navegación, seleccione Usuarios.
3. Seleccione el nombre del usuario para el que quiera habilitar MFA y, a continuación, elija la pestaña Security credentials (Credenciales de seguridad).
4. Al lado de Assigned MFA device (Dispositivo MFA asignado), seleccione Manage (Administrar).
5. Siga las instrucciones del asistente para configurar los dispositivos con MFA en consecuencia. Para obtener más información, consulte Habilitación de los dispositivos con MFA para los usuarios en AWS (documentación de IAM).

ACCT.06: aplicar una política de contraseñas

Los usuarios inician sesión en el AWS Management Console proporcionando las credenciales de inicio de sesión y se recomienda la MFA. Exija que las contraseñas se ajusten a una política de contraseñas segura para evitar que las descubran mediante ataques de fuerza bruta o ingeniería social.

A fin de obtener más información sobre las recomendaciones más recientes para las contraseñas seguras, consulte Guía de políticas de contraseñas en el sitio web de Center for Internet Security (CIS).

En el caso de los usuarios de IAM, puede configurar los requisitos de contraseña en una política de contraseñas de IAM personalizada. Para obtener más información, consulte Configuración de una política de contraseñas de la cuenta (documentación de IAM).

Para crear una política de contraseñas personalizada

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en. https://console.aws.amazon.com/iam
2. En el panel de navegación, elija Configuración de cuenta.
3. En la sección Password policy (Política de contraseñas), elija Change password policy (Cambiar política de contraseñas).
4. Seleccione las opciones que desea aplicar a su política de contraseñas y, a continuación, elija Guardar cambios.

ACCT.07 — Entregue CloudTrail los registros en un bucket S3 protegido

Las acciones realizadas por los usuarios, los roles y los servicios de tu AWS cuenta se registran como eventos en AWS CloudTrail. CloudTrail está activado de forma predeterminada y, en la CloudTrail consola, puedes acceder a la información del historial de eventos de 90 días. Para ver, buscar, descargar, archivar, analizar y responder a la actividad de la cuenta en toda su AWS infraestructura, consulte Visualización de eventos con el historial de CloudTrail eventos (CloudTrail documentación).

Para conservar el CloudTrail historial más allá de 90 días con datos adicionales, debe crear una nueva ruta que envíe los archivos de registro a un depósito de Amazon Simple Storage Service

(Amazon S3) para todos los tipos de eventos. Cuando crea una ruta en la CloudTrail consola, crea una ruta multirregional.

Para crear un sendero que entregue los registros de todos los usuarios Regiones de AWS a un depósito de S3

1. Cree una ruta (CloudTrail documentación). En la página de Elegir eventos de registro, realice lo siguiente:

    a. En la Actividad de la API, elija los Lectura y Escritura.

    b. En los entornos de preproducción, elija Excluir eventos de AWS KMS . Esto excluye todos los AWS Key Management Service (AWS KMS) eventos de tu ruta. AWS KMS lee acciones como `EncryptDecrypt`, y `GenerateDataKey` puede generar un gran volumen de eventos.

    En entornos de producción, elija registrar eventos de administración de Escritura y desactive la casilla de verificación de Excluir eventos de AWS KMS . Esto excluye los eventos de AWS KMS lectura de gran volumen, pero sigue registrando los eventos de escritura relevantes, como `DisableDelete`, y. `ScheduleKey` Estas son las configuraciones de AWS KMS registro mínimas recomendadas para un entorno de producción.

2. El nuevo registro de seguimiento aparece en la página Trails. En unos 15 minutos, CloudTrail publica los archivos de registro que muestran las llamadas a la interfaz de programación de AWS aplicaciones (API) realizadas en su cuenta. Puede ver los archivos de registro del bucket de S3 especificado.

Para ayudar a proteger los depósitos de S3 en los que se almacenan los archivos de CloudTrail registro

1. Revise la política de buckets de Amazon S3 (CloudTrail documentación) para todos y cada uno de los buckets en los que almacene archivos de registro y ajústela según sea necesario para eliminar cualquier acceso innecesario.
2. Como práctica recomendada de seguridad, asegúrese de agregar de forma manual una clave de condición `aws:SourceArn` a la política de bucket. Para obtener más información, consulte Crear o actualizar un bucket de Amazon S3 para almacenar los archivos de registro de una organización (CloudTrail documentación).
3. Habilitar la eliminación de la MFA (documentación de Amazon S3).

ACCT.08: evitar el acceso público a buckets de S3 privados

De forma predeterminada, solo el usuario raíz del principal de IAM Cuenta de AWS y el principal de IAM, si se usa, tienen permisos para leer y escribir en los buckets de Amazon S3 creados por ese principal. A las demás entidades principales de IAM se les concede acceso mediante políticas basadas en identidades, y las condiciones de acceso se pueden aplicar mediante una política de bucket. Puede crear políticas de bucket que concedan al público en general acceso al bucket, un bucket público.

Los buckets que se crearon a partir del 28 de abril de 2023 cuentan con la configuración del Bloqueo de acceso público habilitada de forma predeterminada. En el caso de los buckets que se crearon antes de esta fecha, los usuarios podrían configurar mal la política de bucket y conceder acceso al público sin intención. Puede evitar este error de configuración al habilitar la configuración del Bloqueo de acceso público para cada bucket. Si no tiene casos de uso actuales o futuros para un bucket de S3 público, habilite esta configuración en el Cuenta de AWS nivel. Esta configuración impide las políticas que permiten el acceso público.

Para evitar el acceso público a los buckets de S3

- Configurar los ajustes del bloqueo de acceso público para los buckets de S3 (documentación de Amazon S3).

AWS Trusted Advisor genera un resultado amarillo para los buckets de S3 que permiten el acceso público a listas o de lectura y genera un resultado rojo para los buckets que permiten subir o eliminar archivos de forma pública. Como referencia, siga el control ACCT.12: monitorear y resolver los problemas de alto riesgo mediante el uso de Trusted Advisor para identificar y corregir los buckets mal configurados. Los bucket de S3 de acceso público también se indican en la consola de Amazon S3.

ACCT.09: eliminar las VPC, las subredes y los grupos de seguridad no utilizados

Para reducir la posibilidad de que se produzcan problemas de seguridad, elimine o desactive los recursos que no se utilicen. En una AWS cuenta nueva, de forma predeterminada, se crea automáticamente una nube privada virtual (VPC) en cada una Región de AWS, lo que le permite asignar direcciones IP públicas en subredes públicas. Sin embargo, si no se necesitan estas VPC, existe el riesgo de una exposición no intencionada de los recursos.

Si no se utilizan, elimine las VPC predeterminadas en todas las regiones, no solo en las regiones en las que podría implementar cargas de trabajo. Al eliminar una VPC, también se eliminan sus componentes, como las subredes y los grupos de seguridad.

> **Note**
>
> Puede ver todas las regiones y VPC en la consola de Amazon EC2 Global View en https://console.aws.amazon.com/ec2globalview/home. Para obtener más información, consulte Enumerar y filtrar recursos entre regiones mediante Amazon EC2 Global View (documentación de Amazon EC2).

Para eliminar las VPC predeterminadas no utilizadas

1. Eliminar la VPC (documentación de Amazon VPC).
2. Si es necesario, repita la operación para las VPC en otras regiones.

ACCT.10 — Configure AWS Budgets para controlar sus gastos

AWS Budgets habilite el monitoreo de los costos y el uso mensuales con notificaciones cuando se prevea que los costos superarán los umbrales objetivo. Las notificaciones de costos previstos pueden proporcionar una indicación de una actividad inesperada, lo que proporciona una defensa adicional además de otros sistemas de monitoreo, como AWS Trusted Advisor Amazon GuardDuty. Supervisar y comprender AWS los costes también forma parte de una buena higiene operativa.

Para establecer un presupuesto en AWS Budgets

- Cree un presupuesto de costes (AWS Budgets documentación).

ACCT.11 — Habilita y responde a las notificaciones GuardDuty

Amazon GuardDuty es un servicio de detección de amenazas que monitorea continuamente los comportamientos malintencionados o no autorizados para ayudar a proteger tus AWS cuentas, cargas de trabajo y datos. Cuando detecta actividades inesperadas y potencialmente maliciosas, GuardDuty proporciona datos de seguridad detallados para garantizar su visibilidad y remediarlos. GuardDuty puede detectar amenazas como la actividad minera de criptomonedas, el acceso desde los clientes y retransmisores de Tor, los comportamientos inesperados y las credenciales

de IAM comprometidas. Activa GuardDuty los hallazgos y responde a ellos para detener posibles comportamientos malintencionados o no autorizados en tu AWS entorno. Para obtener más información sobre los hallazgos en GuardDuty, consulte Buscar tipos (GuardDuty documentación).

Puedes usar Amazon CloudWatch Events para configurar notificaciones automáticas cuando se GuardDuty crea una búsqueda o cuando la búsqueda cambia. En primer lugar, debe configurar un tema de Amazon Simple Notification Service (Amazon SNS) y agregar puntos de conexión o direcciones de correo electrónico al tema. A continuación, configura un CloudWatch evento para GuardDuty los hallazgos y la regla de eventos notifica a los puntos de enlace en el tema Amazon SNS.

Para activar las notificaciones GuardDuty GuardDuty

1. Habilita Amazon GuardDuty (GuardDuty documentación).
2. Cree una regla de CloudWatch eventos para notificarle los GuardDuty hallazgos (GuardDutydocumentación).

ACCT.12: monitorear y resolver los problemas de alto riesgo mediante el uso de Trusted Advisor

AWS Trusted Advisor analiza pasivamente su AWS infraestructura para detectar problemas de alto riesgo o alto impacto relacionados con la seguridad, el rendimiento, el coste y la fiabilidad. Brinda información detallada sobre los recursos afectados y las recomendaciones de corrección. Para obtener una lista completa de las comprobaciones y descripciones, consulte la referencia de AWS Trusted Advisor comprobación (documentación)Trusted Advisor .

Revise Trusted Advisor los hallazgos de forma periódica y solucione los problemas según sea necesario. Si tienes los planes AWS Business Support o Enterprise Support, puedes suscribirte a un correo electrónico de información semanal. Para obtener más información, consulte Configurar las preferencias de notificación (documentación de AWS Support).

Para ver los problemas en Trusted Advisor

- Revise cada categoría de cheques según las instrucciones de Ver categorías de cheques (AWS Support documentación). Como mínimo, recomendamos revisar los temas de acción recomendada, que se encuentran en rojo.

Protección de las cargas de trabajo

Los controles y las recomendaciones de esta sección lo ayudan a proteger las cargas de trabajo que se ejecutan en AWS, a medida que las crea. Se enfocan en las prácticas de seguridad para administrar los secretos de las aplicaciones y el alcance del acceso, minimizar las rutas de acceso a los recursos privados y utilizar el cifrado a fin de proteger los datos en tránsito y en reposo.

Esta sección contiene los siguientes temas:

WKLD.01: utilizar los roles de IAM para los permisos del entorno de computación

En AWS Identity and Access Management (IAM), un rol representa un conjunto de permisos que puede asumir una persona o un servicio durante un periodo configurable. El uso de roles

elimina la necesidad de almacenar o administrar las credenciales a largo plazo, lo que reduce de forma considerable la posibilidad de que se produzcan usos no deseados. Asigne un rol de IAM directamente a las instancias de Amazon Elastic Compute Cloud (Amazon EC2), servicios y tareas de AWS Fargate, funciones de AWS Lambda y otros servicios de computación de AWS siempre que sean compatibles. Las aplicaciones que utilizan un SDK de AWS y que se ejecutan en estos entornos de computación utilizan de forma automática las credenciales del rol de IAM para la autenticación.

El enfoque y las instrucciones a fin de utilizar los roles de IAM para cada servicio se encuentran en la Documentación de AWS del servicio. Por ejemplo, consulte lo siguiente:

- Roles de IAM para Amazon EC2 (documentación de Amazon EC2)
- Roles de IAM para tareas (documentación de Amazon Elastic Container Service)
- Rol de ejecución de Lambda (documentación de Lambda)

WKLD.02: restringir el alcance del uso de las credenciales con permisos y políticas basadas en recursos

Las políticas son objetos que pueden definir los permisos o especificar las condiciones de acceso. Existen dos tipos principales de políticas:

- Las políticas basadas en identidades se adjuntan a las entidades principales y definen cuáles son los permisos de la entidad principal en el entorno de AWS.
- Las políticas basadas en recursos se adjuntan a un recurso, como un bucket de Amazon Simple Storage Service (Amazon S3) o un punto de conexión de nube privada virtual (VPC). Estas políticas especifican a qué entidades principales se les permite el acceso, las acciones compatibles y cualquier otra condición que deba cumplirse.

Para que una entidad principal pueda acceder a un recurso y realizar una acción contra un recurso, debe tener el permiso otorgado en su política basada en identidades y cumplir las condiciones de la política basada en recursos. Para obtener más información, consulte Políticas basadas en identidades y políticas basadas en recursos (documentación de IAM).

Las condiciones recomendadas para las políticas basadas en recursos incluyen:

- Restrinja el acceso solo a las entidades principales de una organización específica (definida en AWS Organizations) mediante la condición `aws:PrincipalOrgID`.

- Restrinja el acceso al tráfico que se origina en una VPC específica o un punto de conexión de VPC mediante las condiciones `aws:SourceVpc` o `aws:SourceVpce`, respectivamente.
- Permita o deniegue el tráfico en función de la dirección IP de origen mediante una condición `aws:SourceIp`.

A continuación, se muestra un ejemplo de una política basada en recursos que utiliza la condición `aws:PrincipalOrgID` para permitir que solo las entidades principales en la organización **<o-xxxxxxxxxxx>** accedan al bucket de S3 **<bucket-name>**:

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"AllowFromOrganization",
       "Effect":"Allow",
       "Principal":"*",
       "Action":"s3:*",
       "Resource":"arn:aws:s3:::<bucket-name>/*",
       "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"<o-xxxxxxxxxxx>"}
       }
     }
   ]
}
```

WKLD.03: utilizar secretos efímeros o un servicio de administración de secretos

Los secretos de las aplicaciones consisten principalmente en credenciales, como pares de claves, tokens de acceso, certificados digitales y credenciales de inicio de sesión. La aplicación utiliza estos secretos para acceder a otros servicios de los que depende, como una base de datos. Para ayudar a proteger estos secretos, recomendamos que sean efímeros (es decir, se generan en el momento de la solicitud y son de corta duración, como en el caso de los roles de IAM) o que se recuperen de un servicio de administración de secretos. Esto evita la exposición accidental por mecanismos menos seguros, como que se conserven en archivos de configuración estáticos. Esto también facilita la promoción del código de las aplicaciones desde los entornos de desarrollo hasta los de producción.

En el caso de un servicio de administración de secretos, recomendamos utilizar una combinación del Almacén de parámetros, una capacidad de AWS Systems Manager, y AWS Secrets Manager:

- Utilice el Almacén de parámetros para administrar los secretos y otros parámetros que son pares clave-valor individuales, basados en cadenas, de longitud total corta y de acceso frecuente. Utilice una clave de AWS Key Management Service (AWS KMS) para cifrar el secreto. El almacenamiento de parámetros en el nivel estándar del Almacén de parámetros es gratuito. Para obtener más información sobre los niveles de parámetros, consulte Administración de niveles de parámetros (documentación de Systems Manager).
- Utilice Secrets Manager para almacenar los secretos que se encuentren en forma de documento (como varios pares clave-valor relacionados), que pesen más de 4 KB (como los certificados digitales) o que se beneficiarían de la rotación automática.

Puede utilizar las API del Almacén de parámetros para recuperar los secretos que se almacenan en Secrets Manager. Esto le permite estandarizar el código de su aplicación cuando utiliza una combinación de ambos servicios.

Para administrar secretos en el Almacén de parámetros

1. Crear una clave de AWS KMS simétrica (documentación de AWS KMS).
2. Crear un parámetro SecureString (documentación de Systems Manager). Los secretos en el Almacén de parámetros utilizan el tipo de datos `SecureString`.
3. En su aplicación, recupere un parámetro del Almacén de parámetros mediante el SDK de AWS para su lenguaje de programación. Para ver un ejemplo en Java, consulte GetParameter.java (AWS Code Sample Catalog).

Para administrar los secretos en Secrets Manager

1. Crear un secreto (documentación de Secrets Manager).
2. Recuperar secretos de AWS Secrets Manager en código (documentación de Secrets Manager).

   Es importante leer Utilizar bibliotecas de almacenamiento en caché del lado del cliente de AWS Secrets Manager para mejorar la disponibilidad y la latencia a la hora de utilizar los secretos (publicación de blog de AWS). El uso de los SDK del lado del cliente, que ya tienen implementadas las prácticas recomendadas, debería acelerar y simplificar el uso y la integración de Secrets Manager.

WKLD.04: evitar que se expongan los secretos de las aplicaciones

Durante el desarrollo local, los secretos de las aplicaciones pueden almacenarse en archivos de configuración o código locales y guardarse de forma accidental en los repositorios de código fuente. Los repositorios no seguros alojados en proveedores de servicios públicos pueden estar sujetos al acceso no autorizado y al posterior descubrimiento de estos secretos. Utilice las herramientas disponibles para evitar que se consulten los secretos. Incorpore comprobaciones de los secretos expuestos como parte de sus procesos de revisión de código manual.

Algunas herramientas habituales que pueden evitar que los secretos de las aplicaciones se guarden en los repositorios de código fuente son:

- Gitleaks (repositorio de GitHub)
- Whispers (repositorio de GitHub)
- detect-secrets (repositorio de GitHub)
- git-secrets (repositorio de GitHub)
- TruffleHog (repositorio de GitHub)

WKLD.05: detectar y corregir los secretos expuestos

En WKLD.03: utilizar secretos efímeros o un servicio de administración de secretos y WKLD.04: evitar que se expongan los secretos de las aplicaciones, adopta medidas para proteger los secretos. En este control, implementa una solución que pueda detectar si los secretos han eludido estas medidas de prevención y puede corregir según corresponda.

El Revisor de Amazon CodeGuru detecta los secretos de las aplicaciones en el código fuente y ofrece un mecanismo para corregir y publicar los secretos detectados en Secrets Manager. También se brinda el código de la aplicación para recuperar el secreto de Secrets Manager. Realice un análisis de costo y beneficio para determinar si esta solución es adecuada para su empresa. Como alternativa, algunas de las soluciones de código abierto en WKLD.04: evitar que se expongan los secretos de las aplicaciones ofrecen la capacidad de detección de los secretos existentes.

Para configurar la integración del Revisor de CodeGuru con Secrets Manager

- Utilizar el Revisor de CodeGuru para identificar secretos codificados y AWS Secrets Manager a fin de protegerlos (tutorial y publicación de blog de AWS).

WKLD.06: utilizar Systems Manager en lugar de SSH o RDP

Las subredes públicas, que tienen una ruta predeterminada que apunta a una puerta de enlace de Internet, representan intrínsecamente un riesgo de seguridad mayor que las subredes privadas, que no tienen acceso a Internet. Puede ejecutar instancias de EC2 en subredes privadas y utilizar la función de Session Manager de AWS Systems Manager para acceder de forma remota a las instancias a través de la AWS Command Line Interface (AWS CLI) o AWS Management Console. Luego, puede utilizar la AWS CLI o consola para iniciar una sesión que se conecte a la instancia a través de un túnel seguro, lo que evita la necesidad de administrar las credenciales adicionales que se utilizan para Secure Shell (SSH) o el protocolo de escritorio remoto (RDP) de Windows.

Utilice Session Manager en lugar de ejecutar instancias de EC2 en subredes públicas, ejecutar cajas de conexiones o ejecutar hosts bastión.

Para configurar Session Manager

1. Asegúrese de que la instancia de EC2 utilice el sistema operativo de Imágenes de máquina de Amazon (AMI) más reciente, como Amazon Linux 2 o Ubuntu. AWS Systems Manager Agent (SSM Agent) se encuentra preinstalado en la AMI.
2. Asegúrese de que la instancia tenga conectividad, ya sea a través de una puerta de enlace de Internet o de puntos de conexión de VPC, a estas direcciones (al reemplazar **`<region>`** por la Región de AWS apropiada):
    a. Ec2messages.<region>.amazonaws.com
    b. ssm.<region>.amazonaws.com
    c. ssmmessages.<region>.amazonaws.com
3. Adjunte `AmazonSSMManagedInstanceCore`, la política administrada por AWS, al rol de IAM que se encuentra asociado a las instancias.

Para obtener más información, consulte Configuración de Session Manager (documentación de Systems Manager).

Para iniciar una sesión

- Iniciar una sesión (documentación de Systems Manager).

WKLD.07: registrar eventos de datos para buckets de S3 con datos confidenciales

De forma predeterminada, AWS CloudTrail registra los eventos de administración, los eventos que crean, modifican o eliminan los recursos de su cuenta. Estos eventos de administración no registran las operaciones de lectura o escritura en objetos individuales de los buckets de Amazon Simple Storage Service. Durante un incidente de seguridad, es importante registrar el acceso o el uso no autorizado de los datos a nivel de registro u objeto individual. Utilice CloudTrail para registrar los eventos de datos de cualquier bucket de S3 que almacene datos confidenciales o fundamentales para la empresa, con fines de detección y auditoría.

> **Note**
>
> Se aplican cargos adicionales para registrar eventos de datos. Para obtener más información, consulte Precios de AWS CloudTrail.

A fin de registrar eventos de datos para registros de seguimiento

1. Iniciar sesión en la AWS Management Console y abrir la consola de CloudTrail en https://console.aws.amazon.com/cloudtrail/
2. En el panel de navegación, elija Trails (Registros de seguimiento) y, a continuación, elija un nombre de registro de seguimiento.
3. En Detalles generales, elija Editar para cambiar la siguiente configuración. No puede cambiar el nombre de un registro de seguimiento.
    a. En Eventos de datos, elija Editar.
    b. En Data event source (Fuente de evento de datos), elija S3.
    c. En Todos los buckets de S3 actuales y futuros, anule la selección de Lectura y Escritura.
    d. En Selección de bucket individual, busque un bucket en el que registrar los eventos de datos. En esta ventana puede seleccionar varios buckets. Elija Add bucket (Agregar bucket) para registrar eventos de datos en más buckets. Elija registrar eventos de Read (Lectura), como `GetObject`, Write (Escritura), como `PutObject`, o de ambos.
    e. Elija Update trail (Actualizar registro de seguimiento).

WKLD.08: cifrar volúmenes de Amazon EBS

Aplique el cifrado de los volúmenes de Amazon Elastic Block Store (Amazon EBS) como comportamiento predeterminado en su cuenta de AWS. Los volúmenes cifrados tienen el mismo rendimiento de operaciones de entrada/salida por segundo (IOPS) que los volúmenes no cifrados, con un efecto mínimo en la latencia. Esto evita que se regeneren los volúmenes en una fecha posterior por motivos de conformidad o por otros motivos. A fin de obtener más información, consulte las Prácticas recomendadas más conocidas para el cifrado de Amazon EBS(publicación de blog de AWS).

Para cifrar volúmenes de Amazon EBS

- Habilitar el cifrado de forma predeterminada (documentación de Amazon EC2).

WKLD.09: cifrar las bases de datos de Amazon RDS

Al igual que WKLD.08: cifrar volúmenes de Amazon EBS, habilite el cifrado de las bases de datos de Amazon Relational Database Service (Amazon RDS). Este cifrado se realiza en el nivel de volumen subyacente y tiene el mismo rendimiento de IOPS que los volúmenes no cifrados, con un efecto mínimo en la latencia. Para obtener más información, consulte Información general del cifrado de los recursos de Amazon RDS (documentación de Amazon RDS).

Para cifrar una instancia de base de datos de RDS

- Cifrar una instancia de base de datos (documentación de Amazon RDS).

WKLD.10: implementar recursos privados en subredes privadas

Implemente recursos que no requieran acceso directo a Internet, como instancias de EC2, bases de datos, colas, almacenamiento en caché u otra infraestructura, en una subred privada de VPC. Las subredes privadas no tienen una ruta declarada en su tabla de enrutamiento a una puerta de enlace de Internet adjuntada y no pueden recibir tráfico de Internet. El tráfico que se origina en una subred privada con destino a Internet debe someterse a la traducción de direcciones de red (NAT) a través de una puerta de enlace de NAT de AWS administrada o una instancia de EC2 que ejecute procesos de NAT en una subred pública. Para obtener más información sobre el aislamiento de la red, consulte Seguridad de la infraestructura en Amazon VPC (documentación de Amazon VPC).

Utilice las siguientes prácticas al crear subredes y recursos privados:

- Al crear una subred privada, deshabilite Asignar automáticamente una dirección IPv4.
- Al crear instancias de EC2 privadas, deshabilite Asignar automáticamente una IP pública. Esto evita que se asigne una IP pública si la instancia se implementa de forma no intencionada en una subred pública debido a un error de configuración.

Si es necesario, se especifica la subred de un recurso como parte de su configuración. Puede implementar una VPC que siga las prácticas recomendadas mediante el Inicio rápido de la arquitectura de VPC modular y escalable (Inicios rápidos de AWS).

WKLD.11: restringir el acceso a la red mediante grupos de seguridad

Utilice los grupos de seguridad para controlar el tráfico a las instancias de EC2, las bases de datos de RDS y otros recursos compatibles. Los grupos de seguridad actúan como un firewall virtual que se puede aplicar a cualquier grupo de recursos relacionados a fin de definir de forma coherente las reglas que permitan el tráfico entrante y saliente. Además de las reglas basadas en las direcciones IP y los puertos, los grupos de seguridad admiten reglas para permitir el tráfico desde los recursos asociados a otros grupos de seguridad. Por ejemplo, un grupo de seguridad de base de datos puede tener reglas que solo permitan el tráfico procedente de un grupo de seguridad de servidores de aplicaciones.

De forma predeterminada, los grupos de seguridad permiten todo el tráfico saliente, pero no el tráfico entrante. Se puede eliminar la regla de tráfico saliente o configurar reglas adicionales que se agreguen para restringir el tráfico saliente y permitir el tráfico entrante. Si el grupo de seguridad no tiene reglas entrantes, no se permitirá el tráfico saliente que proceda de esta instancia. Para obtener más información, consulte Control del tráfico hacia los recursos mediante grupos de seguridad (documentación de Amazon VPC).

En el siguiente ejemplo, hay tres grupos de seguridad que controlan el tráfico desde un equilibrador de carga de aplicación a las instancias de EC2 que se conectan a una base de datos de Amazon RDS para MySQL.

Security group (Grupo de seguridad)	Reglas de entrada	Reglas de salida
Grupo de seguridad del equilibrador de carga de aplicación	Descripción: permitir el tráfico HTTPS desde cualquier lugar Tipo: HTTPS Origen: cualquier IPv4 (0.0.0.0/0)	Descripción: permitir todo el tráfico a cualquier lugar Tipo: todo el tráfico Destino: cualquier IPv4 (0.0.0.0/0)
Grupo de seguridad de la instancia de EC2	Descripción: permitir el tráfico HTTP desde el equilibrador de carga de aplicación Type (Tipo): HTTP Origen: grupo de seguridad del equilibrador de carga de aplicación	Descripción: permitir todo el tráfico a cualquier lugar Tipo: todo el tráfico Destino: cualquier IPv4 (0.0.0.0/0)
Grupo de seguridad de la base de datos de RDS	Descripción: permitir el tráfico de MySQL desde la instancia de EC2 Tipo: MySQL Origen: grupo de seguridad de la instancia de EC2	Sin reglas de salida

WKLD.12: utilizar puntos de conexión de VPC para acceder a los servicios compatibles

En las VPC, los recursos que necesitan acceder a AWS u otros servicios externos requieren una ruta a Internet (`0.0.0.0/0`) o a la dirección IP pública del servicio de destino. Utilice los puntos de conexión de VPC para habilitar una ruta IP privada desde su VPC hasta AWS u otros servicios, lo que evita la necesidad de utilizar una puerta de enlace de Internet, un dispositivo de NAT, una conexión de red privada virtual (VPN) o una conexión de AWS Direct Connect.

Los puntos de conexión de VPC admiten la conexión de políticas y grupos de seguridad para controlar aún más el acceso a un servicio. Por ejemplo, puede escribir una política de puntos de conexión de VPC para Amazon DynamoDB que solo permita acciones a nivel de elemento e impida acciones a nivel de tabla para todos los recursos de la VPC, independientemente de su propia política de permisos. También puede escribir una política de bucket de S3 para solo permitir las solicitudes que se originen en un punto de conexión de VPC específico y denegar todos los demás accesos externos. Un punto de conexión de VPC también puede tener una regla de grupo de seguridad que, por ejemplo, restrinja el acceso solo a las instancias de EC2 que se encuentren asociadas a un grupo de seguridad específico de la aplicación, como el nivel de lógica empresarial de una aplicación web.

Existen diferentes tipos de puntos de conexión de VPC. Accede a la mayoría de los servicios mediante un punto de conexión de interfaz de VPC. Se accede a DynamoDB mediante un punto de conexión de puerta de enlace. Amazon S3 admite puntos de conexión de puerta de enlace y de interfaz. Se recomiendan los puntos de conexión de puerta de enlace para las cargas de trabajo en una sola cuenta y región de AWS, además no tienen un cargo adicional. Se recomiendan los puntos de conexión de interfaz si se requiere un acceso más extensible, por ejemplo, a un bucket de S3 desde otras VPC, desde redes en las instalaciones o desde otras Regiones de AWS. Los puntos de conexión de interfaz conllevan un cargo por tiempo de funcionamiento por hora y por procesamiento de datos por GB, ambos inferiores a los cargos correspondientes por enviar los datos a `0.0.0.0/0` mediante la puerta de enlace de NAT de AWS.

Consulte los siguientes recursos para obtener información adicional sobre el uso de los puntos de conexión de VPC:

- A fin de obtener más información sobre la selección entre los puntos de conexión de puerta de enlace y de interfaz para Amazon S3, consulte Elección de su estrategia de puntos de conexión de VPC para Amazon S3 (publicación de blog de AWS).
- Crear un punto de conexión de interfaz (documentación de Amazon VPC).
- Crear un punto de conexión de puerta de enlace (documentación de Amazon VPC).
- Para ver ejemplos de políticas de bucket de S3 que restringen el acceso a una VPC específica o un punto de conexión de VPC, consulte Restricción del acceso a una VPC específica (documentación de Amazon S3).
- A fin de ver ejemplos de políticas de puntos de conexión de DynamoDB que restringen las acciones, consulte Políticas de punto de conexión para DynamoDB (documentación de Amazon VPC).

WKLD.13: requerir HTTPS para todos los puntos de conexión web públicos

Requiera HTTPS para aportar mayor credibilidad a sus puntos de conexión web, permita que sus puntos de conexión utilicen certificados a fin de demostrar su identidad, y confirme que todo el tráfico entre su punto de conexión y los clientes conectados se encuentre cifrado. En el caso de los sitios web públicos, esto ofrece el beneficio adicional de tener una mejor clasificación en los motores de búsqueda.

Muchos servicios de AWS brindan puntos de conexión web públicos para sus recursos, como AWS Elastic Beanstalk, Amazon CloudFront, Amazon API Gateway, Elastic Load Balancing y AWS Amplify. A fin de obtener instrucciones sobre cómo se requiere HTTPS para cada uno de estos servicios, consulte lo siguiente:

- Elastic Beanstalk (documentación de Elastic Beanstalk)
- CloudFront (documentación de CloudFront)
- Equilibrador de carga de aplicación (Centro de conocimientos de AWS)
- Equilibrador de carga clásico (Centro de conocimientos de AWS)
- Amplify (documentación de Amplify)

Los sitios web estáticos que se encuentran en Amazon S3 no admiten HTTPS. A fin de requerir HTTPS para estos sitios web, puede utilizar CloudFront. No es necesario el acceso público a los buckets de S3 que entregan contenido a través de CloudFront.

Para utilizar CloudFront a fin de entregar un sitio web estático alojado en Amazon S3

1. Utilizar CloudFront para entregar un sitio web estático alojado en Amazon S3 (Centro de conocimientos de AWS).
2. Si configura el acceso a un bucket de S3 público, consulte requerir HTTPS entre los lectores y CloudFront (documentación de CloudFront).

   Si configura el acceso a un bucket de S3 privado, consulte restringir el acceso al contenido de Amazon S3 mediante una identidad de acceso de origen (documentación de CloudFront).

Además, configure los puntos de conexión de HTTPS para que requieran protocolos y cifrados modernos de la seguridad de la capa de transporte (TLS), a menos que sea necesaria la

compatibilidad con protocolos anteriores. Por ejemplo, utilice la `ELBSecurityPolicy-FS-1-2-Res-2020-10` o la política más reciente disponible para los oyentes HTTPS del equilibrador de carga de aplicación, en lugar de la `ELBSecurityPolicy-2016-08` predeterminada. Las políticas más actuales requieren como mínimo el uso de TLS 1.2, confidencialidad directa y sistemas de cifrado seguros que sean compatibles con los navegadores web modernos.

A fin de obtener más información sobre las políticas de seguridad disponibles para los puntos de conexión públicos de HTTPS, consulte:

- Políticas de seguridad SSL predefinidas para los equilibradores de carga clásicos (documentación de Elastic Load Balancing)
- Políticas de seguridad para el equilibrador de carga de aplicación (documentación de Elastic Load Balancing)
- Protocolos y cifrados admitidos entre lectores y CloudFront (documentación de CloudFront)

WKLD.14: utilizar servicios de protección de periferia para puntos de conexión públicos

En lugar de entregar el tráfico directamente desde los servicios de computación, como los contenedores o instancias de EC2, utilice un servicio de protección de periferia. Esto ofrece una capa de seguridad adicional entre el tráfico entrante de Internet y los recursos que prestan servicio a ese tráfico. Estos servicios pueden filtrar el tráfico no deseado, aplicar el cifrado y aplicar el enrutamiento u otras reglas, como el equilibrio de carga, antes de que el tráfico llegue a sus recursos internos.

Los servicios de AWS que pueden aportar una protección de puntos de conexión públicos incluyen AWS WAF, CloudFront, Elastic Load Balancing, API Gateway y Amplify Hosting. Ejecute servicios basados en VPC, como Elastic Load Balancing, en una subred pública como proxy de los recursos de servicios web que se ejecutan en una subred privada.

CloudFront, API Gateway y Amazon Route 53 ofrecen protección contra los ataques de denegación de servicio distribuido (DDoS) de capa 3 y 4 sin costo alguno, y AWS WAF puede proteger contra los ataques de capa 7.

Las instrucciones para comenzar a utilizar cada uno de estos servicios se encuentran aquí:

- Introducción a AWS WAF (sitio web de AWS)
- Introducción a Amazon CloudFront (documentación de CloudFront)

- Introducción a Elastic Load Balancing (documentación de Elastic Load Balancing)
- Introducción a API Gateway (documentación de API Gateway)
- Introducción a Amplify Hosting(documentación de Amplify)

WKLD.15: definir los controles de seguridad en las plantillas e implementarlos mediante prácticas de CI/CD

La infraestructura como código (IaC) es la práctica de definir todos sus recursos y configuraciones de los servicios de AWS en las plantillas y el código que utiliza las canalizaciones de integración y entrega continua (CI/CD), las mismas canalizaciones que utiliza para implementar las aplicaciones de software. Los servicios de IaC, como AWS CloudFormation, admiten políticas basadas en identidades y recursos de IAM y admiten servicios de seguridad AWS, como Amazon GuardDuty, AWS WAF y Amazon VPC. Registre estos artefactos como plantillas de IaC, guarde las plantillas en un repositorio de código fuente y, a continuación, impleméntelas mediante canalizaciones de CI/CD.

A menos que se requiera lo contrario, confirme las políticas de permisos de las aplicaciones con el código de la aplicación en el mismo repositorio y administre las políticas generales de recursos y las configuraciones de los servicios de seguridad en repositorios de código y canalizaciones de implementación independientes.

Para obtener más información sobre cómo comenzar con la IaC en AWS, consulte la documentación de AWS Cloud Development Kit (AWS CDK).

Colaboradores

Los colaboradores de este documento son:

- Jay Michael, arquitecto de soluciones principal
- Cole Calistra, arquitecto de soluciones principal
- Justin Plock, arquitecto de soluciones principal
- Faisal Farooq, arquitecto de soluciones
- Michael Nguyen, arquitecto de soluciones sénior
- Ritik Khatwani, arquitecto de soluciones sénior
- Paul Hawkins, encargado de seguridad de la información (CISO)

Un agradecimiento especial a las siguientes personas, que también ayudaron con la orientación y la revisión:

- Robert Put
- Mike Sullivan
- Bob Lee III

Historial de documentos

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

Cambio	Descripción	Fecha
Configuración del bucket de Amazon S3	Hemos actualizado la sección ACCT.08: evitar el acceso público a buckets de S3 privados para reflejar que los buckets de Amazon S3 creados después del 28 de abril de 2023 tienen habilitad a la configuración del Bloqueo de acceso público de forma predeterminada.	18 de mayo de 2023
Prácticas recomendadas de seguridad de IAM	Hemos actualizado esta guía para alinearla con las prácticas recomendadas de AWS Identity and Access Management (IAM) más recientes. Para obtener más información, consulte Prácticas recomendadas de seguridad en la documenta ción de IAM.	1 de febrero de 2023
Roles de IAM	Encontrará enlaces adicional es a la documentación de Servicio de AWS en la sección WKLD.01: Utilizar los roles de IAM para los permisos del entorno de computación.	22 de septiembre de 2022

Política de contraseñas	Hemos actualizado las recomendaciones sobre las contraseñas seguras para seguir las directrices más recientes de Center for Internet Security (CIS).	10 de mayo de 2022
Publicación inicial	—	13 de abril de 2022

Glosario de las Recomendaciones de AWS

Los siguientes son términos de uso común en las estrategias, guías y patrones que se ofrecen en las Recomendaciones de AWS. 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 la base de datos de Oracle en las instalaciones a Amazon Aurora PostgreSQL-Compatible Edition.
- 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 la base de datos Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle en la 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 el sistema de administración de las 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 de Oracle en las instalaciones a Oracle en una instancia de EC2 en la 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. Este escenario de migración es específico de VMware Cloud en AWS, que permite la compatibilidad de máquinas virtuales (VM) y la portabilidad de cargas de trabajo entre el entorno en las instalaciones y de AWS. Puede utilizar las tecnologías de VMware Cloud Foundation desde los centros de datos en las instalaciones al migrar una infraestructura a VMware Cloud en AWS. Ejemplo: Reubicar el hipervisor que aloja la base de datos de Oracle a VMware Cloud en 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. A fin de obtener más información, consulte ABAC para AWS en la documentación de AWS Identity and Access Management (IAM).

origen de datos fidedigno

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

Zona de disponibilidad

Ubicación diferenciada de una Región de AWS que está aislada de los errores que se producen en otras zonas de disponibilidad y que brinda conectividad de red económica y de baja latencia a otras zonas de disponibilidad de la misma región.

AWS Cloud Adoption Framework (AWS CAF)

Marco de directrices y prácticas recomendadas de AWS para ayudar a las empresas a desarrollar un plan eficiente y eficaz a fin de migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque llamadas perspectivas: empresarial, humana, gobernanza, 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 brinda orientación para el desarrollo, la capacitación y la comunicación de las personas, con el fin de ayudar a preparar 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 Workload Qualification Framework (AWS WQF)

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y brinda 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

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.

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 (documentación)GitHub .

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-ArchitectedAWS.

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.

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 de forma local, antes de que el Servicio de AWS de destino los 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 del CCoE en el Blog de estrategia empresarial en la nube de AWS.

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 siguientes son las cuatro fases por las que suelen pasar las empresas cuando migran a la 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 publicación del blog The Journey Toward Cloud-First & the Stages of Adoption (El camino hacia la nube como prioridad y las etapas de adopción) en el Blog de estrategia empresarial en la nube de AWS. Para obtener información sobre cómo se relacionan con la estrategia de migración de AWS, consulte la Guía de preparación para la migración.

CMDB

Consulte la base de datos de gestión 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 oAWS 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

Campo de IA utilizado por las máquinas para identificar personas, lugares y cosas en imágenes con una precisión igual o superior a la humana. Construido a menudo con modelos de aprendizaje profundo, automatiza la extracción, el análisis, la clasificación y la comprensión de información útil a partir de una sola imagen o una secuencia de imágenes.

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

Una colección de acciones correctivas y reglas de AWS Config que puede reunir para personalizar sus controles de seguridad y conformidad. Puede implementar un paquete de conformidad como una sola entidad en una región y Cuenta de AWS, o en toda una organización, mediante una plantilla YAML. Para obtener más información, consulte Paquetes de conformidad en la documentación de 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.

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 Marco de AWS Well-Architected. 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.

minimización de datos

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

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. Cuando se adopta esta estrategia en AWS, se suman varios controles en diferentes capas de la estructura de AWS Organizations 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 miembro de AWS a fin de administrar las cuentas de la organización y los permisos para 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 de desastres de cargas de trabajo en AWS: Recuperación en la nube en un marco Well-Architected AWS.

DML

Consulte el lenguaje de manipulación de bases de datos.

diseño basado en el dominio

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

DR

Consulte recuperación ante desastres.

detección de deriva

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

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

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 de conexión con AWS PrivateLink y conceder permisos a otras Cuentas de AWS o para entidades principales de 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).

cifrado de sobre

El proceso de cifrar una clave de cifrado con otra clave de cifrado. Para obtener más información, consulte Cifrado de sobre 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 de seguridad de AWS CAF incluyen la administración 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.

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 elNube de AWS, un límite, como una zona de disponibilidadRegión 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 la sección Restringir la distribución geográfica del contenido en la CloudFront documentación.

Flujo de trabajo de Gitflow

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

estrategia de implementación desde cero

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

barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y 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 GuardDutyAWS 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

Una política asociada a una o más entidades principales de IAM que define sus permisos en el entorno de la Nube de AWS.

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

Véase el Internet industrial de las cosas.

infraestructura inmutable

Un modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar, parchear o modificar la infraestructura existente. Las infraestructuras

inmutables son intrínsecamente más consistentes, fiables y predecibles que las infraestructuras mutables. Para obtener más información, consulte las prácticas recomendadas para implementar con una infraestructura inmutable en Well-Architected FrameworkAWS.

VPC entrante (de entrada)

En una arquitectura de varias cuentas de AWS, 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.

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 varias cuentas de AWS, una VPC centralizada que administra las inspecciones del tráfico de red entre VPC (en la misma o en diferentes Regiones de AWS), Internet y las redes en las instalaciones. 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 zona de aterrizaje es un entorno de AWS correctamente diseñado, con varias cuentas, que es 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 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.

servicios gestionados

Servicios de AWSpara 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.

MAP

Consulte Migration Acceleration Program.

mecanismo

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

cuenta de miembro

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

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 Integración de microservicios mediante servicios sin servidor de 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)

Programa de AWS que brinda soporte de consultoría, capacitación y servicios para ayudar a las empresas a construir una base operativa sólida para migrar a la nube y 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 Migration Factory suelen incluir operadores, analistas de negocio y propietarios, 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 las subredes de destino, los grupos de seguridad y las cuentas de AWS.

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: Volver a alojar la migración en Amazon EC2 con AWS Application Migration Service.

Migration Portfolio Assessment (MPA)

Herramienta en línea que brinda información a fin de validar los argumentos comerciales necesarios para migrar a la 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 inicio de sesión) está disponible de forma gratuita para todos los consultores de AWS y los consultores asociados de APN.

Evaluación de la preparación para la migración (MRA)

Proceso que consiste en obtener información sobre el estado de preparación de la nube de una organización, identificar los puntos fuertes y débiles, y elaborar un plan de acción para cerrar las brechas identificadas, mediante 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

Enfoque utilizado para migrar una carga de trabajo a la 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.

MAPA

Consulte la evaluación de la cartera de migración.

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 la 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 la 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.

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.

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.

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

Registro de seguimiento creado por AWS CloudTrail que registra todos los eventos para todas las Cuentas de AWS en una organización en 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 migración de AWS, este marco se denomina aceleración de personas, debido a la velocidad de cambio requerida en 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 es compatible con todos los buckets de S3 en todas las Regiones de AWS, cifrado del servidor con AWS KMS (SSE-KMS), y solicitudes `PUT` y `DELETE` dinámicas 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.

VPC saliente (de salida)

En una arquitectura de varias cuentas de AWS, 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.

política

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

entorno de producción

Consulte entorno.

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.

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

Conjunto de recursos de AWS que se encuentran en un área geográfica. Cada Región de AWS está aislada y es independiente de las demás para ofrecer tolerancia a errores, estabilidad y resistencia. Para obtener más información, consulte Administración de Regiones de AWS en Referencia general de AWS.

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

Ver 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.

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

Ver 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 característica permite el inicio de sesión único (SSO) federado a fin de que los usuarios puedan iniciar sesión en la AWS Management Console o llamar a la API de AWS sin necesidad de crear un usuario de IAM para cada persona 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.

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, consulte la documentación de Secret in the 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. Existen cuatro tipos principales de controles de seguridad: preventivos, de detección, con capacidad de respuesta y proactivos.

refuerzo de la seguridad

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

sistema de información sobre seguridad y administración de eventos (SIEM)

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

automatización de la respuesta de seguridad

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

cifrado del servidor

Cifrado de los datos en su destino, por parte del Servicio de AWS que 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 Políticas de control de servicio en la documentación de AWS Organizations.

punto de enlace de servicio

La URL del punto de entrada para 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

Modelo que describe la responsabilidad que comparte con AWS en cuanto a la conformidad y la seguridad en 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

SPOF

Consulte el punto único de falla.

esquema en forma de estrella

Estructura organizativa de una base de datos que utiliza una tabla de hechos grande para almacenar datos medidos o transaccionales 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.

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 de clave y valor que funcionan como metadatos para organizar los recursos de 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 puerta de enlace de tránsito? en la documentación de AWS Transit Gateway.

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

Concesión de permisos a un servicio que especifique para realizar tareas en su empresa en 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 Uso de AWS Organizations con otros servicios de AWS en la documentación de AWS Organizations.

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 tibios

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.