¿Transición a múltiples Cuentas de AWS

AWS Guía prescriptiva

AWS Guía prescriptiva: ¿Transición a múltiples Cuentas de AWS

Table of Contents

Transición a múltiples Cuentas de AWS

Amazon Web Services (colaboradores)

Mayo de 2024 (historial del documento)

Muchas empresas comienzan su recorrido con una única cuenta de Amazon Web Services (AWS). Varios roles dentro de una empresa utilizan esta cuenta para gestionar la empresa. Los ingenieros desarrollan códigos, los implementan en entornos de desarrollo y prueba y promueven cambios en la producción. Los gerentes de producto consultan los orígenes de datos para recopilar información sobre el rendimiento empresarial. El equipo de ventas realiza demostraciones desde el entorno de producción para atraer nuevos clientes. El equipo de finanzas monitorea los gastos en la nube desde la AWS Billing consola.

Cuando todas estas funciones independientes utilizan una sola función Cuenta de AWS, puede resultar difícil aplicar la mejor práctica de seguridad consistente en aplicar los permisos con menos privilegios, lo que significa conceder solo los permisos mínimos necesarios para realizar el trabajo. En una etapa determinada del desarrollo de una startup, alguien hará la pregunta ¿Todos nuestros ingenieros necesitan acceso a la producción? La respuesta es casi siempre no, pero muchas empresas tienen dificultades para convertir su entorno actual de cuenta única en un entorno de varias cuentas sin ralentizar el negocio.

En esta guía, se incluyen prácticas recomendadas para ayudarlo a pasar de un entorno de una cuenta única a un entorno de varias cuentas. En ella se analizan las decisiones que debe tomar sobre la migración de cuentas, la administración de usuarios, las redes, la seguridad y la arquitectura. Está diseñada para ayudarlo a obtener los resultados deseados con un tiempo de inactividad mínimo o nulo para su empresa y sus operaciones diarias. Esta guía se centra en las siguientes funciones a medida que se realiza la transición de un entorno de una sola cuenta Cuenta de AWS a uno de múltiples cuentas:

- Administración de identidades y control de acceso
- Administración de permisos y acceso
- La conectividad de red
- Respuesta a un incidente de seguridad
- Copias de seguridad
- Migración de cuenta

- Migración de recursos
- Consideraciones sobre la facturación

Para obtener más información acerca de las capacidades, consulte Cloud Foundation en AWS.

Esta guía se ajusta a los recursos existentes relacionados con este tema, como la base de seguridad de las AWS empresas emergentes (AWS SSB), el documento técnico sobre cómo organizar su AWS entorno con varias cuentas, la arquitectura de referencia de AWS seguridad (AWS SRA) y el documento técnico Establir su base en la nube. AWS Debe seguir utilizando esos recursos para obtener una orientación más específica que no se incluye en esta guía.

Destinatarios previstos

Esta guía es la más adecuada para las empresas que desean o necesitan hacer la transición a varias Cuentas de AWS. En el caso de las empresas emergentes, esta necesidad suele surgir cuando han encontrado un producto adecuado para el mercado, han conseguido una ronda de financiación y están empezando a contratar distintas disciplinas de ingeniería, como la infraestructura, las operaciones de desarrollo () o la seguridad. DevOps

Aunque su empresa no esté preparada para realizar esta transición, puede utilizar esta guía para comprender las decisiones que deben tomarse durante la transición y empezar a prepararse.

Resultados empresariales específicos para la transición a una arquitectura de varias cuentas

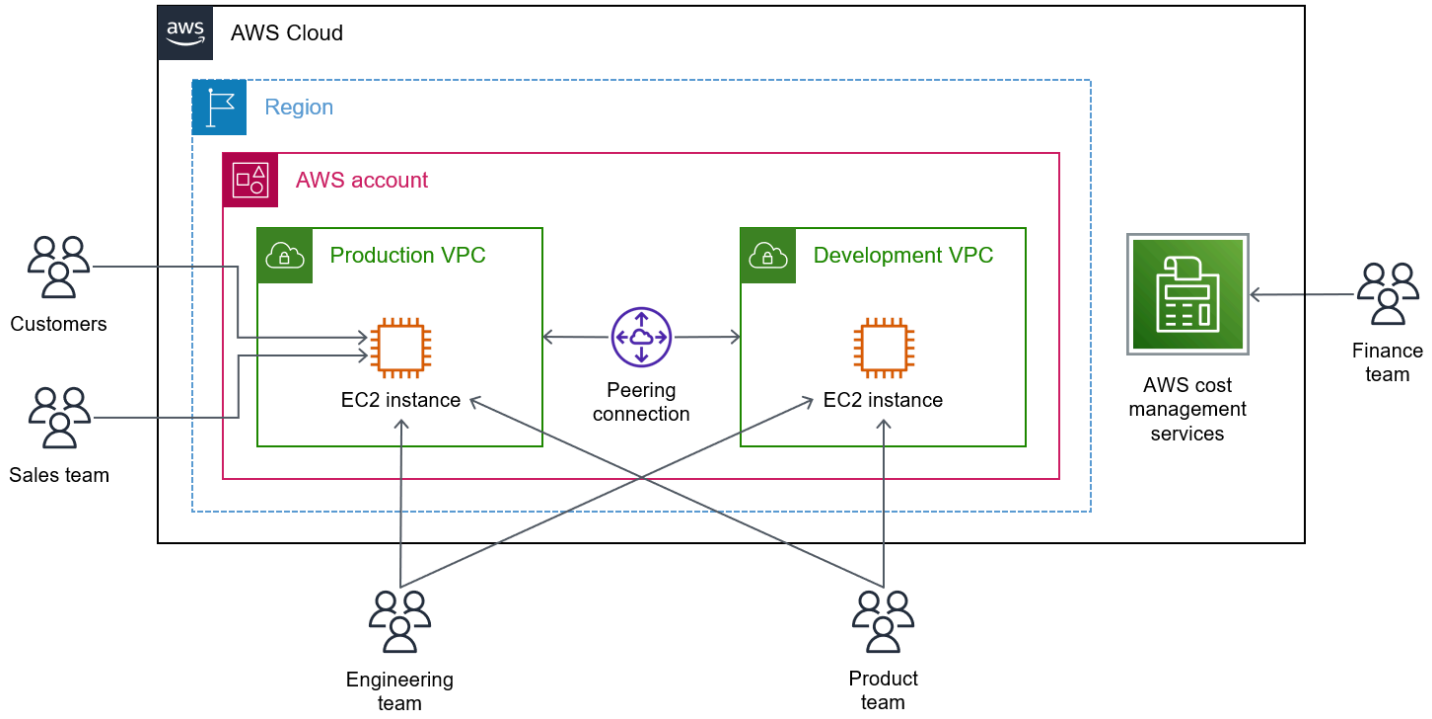
La transición a una arquitectura de varias cuentas suele estar impulsada por la necesidad empresarial de obtener uno o más de los siguientes beneficios:

- Agrupar las cargas de trabajo según el propósito o la propiedad de la empresa
- Aplicar distintos controles de seguridad por entorno
- Restringir el acceso a los datos confidenciales
- Promover la innovación y la agilidad
- Limitar el alcance del impacto de los eventos adversos
- Ser compatible con varios modelos operativos de TI
- Administrar costos
- Distribuir cuotas de Servicio de AWS y límites de frecuencia de solicitudes de API

Para obtener más información sobre las numerosas ventajas de utilizar una arquitectura de varias cuentas, consulte Cómo organizar su entorno de AWS con varias cuentas (documento técnico de AWS) y Directrices para configurar un entorno de buena arquitectura (documentación de AWS Control Tower).

Ejemplo de arquitectura de cuenta única

Como punto de partida, es habitual que las startups o pequeñas empresas utilicen una única Región de AWS y tengan dos nubes privadas virtuales (VPC) que están conectadas por Interconexión de VPC. Cada VPC contiene recursos de computación, como las instancias de Amazon Elastic Compute Cloud (Amazon EC2). El equipo de ingeniería desarrolla el código directamente en la VPC de desarrollo. El equipo de producto revisa los cambios y, a continuación, el equipo de ingeniería los promueve de forma manual a la VPC de producción. El equipo de finanzas tiene acceso a la Cuenta de AWS para que puedan revisar la consola de AWS Billing and Cost Management.



A continuación, se muestran algunos ejemplos de desafíos que una empresa podría experimentar en este entorno:

- Un ingeniero borró por error los datos de producción cuando pensó que estaba accediendo a una base de datos de desarrollo.
- Una demostración de ventas se vio afectada cuando una implementación de producción tardó más de lo esperado.
- Cuando se estaba realizando una prueba de carga del código de desarrollo, la VPC de producción se ralentizó y generó mensajes de error relacionados con la limitación.
- El equipo de finanzas no puede diferenciar los costos de los entornos de producción y desarrollo.
- Al director ejecutivo le preocupa que algunos contratistas externos recién contratados tengan acceso a los datos de los clientes a través de la VPC de producción.
- El equipo de finanzas no puede denegar el acceso a determinados Servicios de AWS que podrían incurrir en altos costos.

La adopción de una estrategia de varias cuentas aborda todos estos desafíos mediante el uso de Cuentas de AWS compartimentadas para separar las cargas de trabajo y el acceso.

Marco fundamental y responsabilidades de seguridad para la transición a una arquitectura de varias cuentas

La información y las prácticas recomendadas en esta guía están diseñadas para complementar las sugerencias existentes de AWS de infraestructura y seguridad. A medida que pasa de una única Cuenta de AWS a varias Cuentas de AWS, es importante asegurarse de que su nueva arquitectura de varias cuentas sea coherente con el Marco de AWS Well-Architected y los principios de Cloud Foundation. Esto lo ayuda a crear y operar un entorno diseñado para ofrecer seguridad, rendimiento y resistencia, a la vez que cumple con los requisitos de gobernanza y las prácticas recomendadas de AWS.

Marco de AWS Well-Architected

El Marco de AWS Well-Architected lo ayuda a crear infraestructuras seguras, de alto rendimiento, resistentes y eficientes para las aplicaciones y cargas de trabajo. Esta guía se ajusta a los pilares Excelencia operativa, Seguridad y Fiabilidad de este marco. 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 una buena arquitectura mediante AWS Well-Architected Tool en su Cuenta de AWS.

Cloud Foundation en AWS

Establecer Cloud Foundation en AWS (documento técnico de AWS) le brinda orientación que lo ayuda a personalizar su entorno de AWS que satisfaga las necesidades de su empresa. Con un enfoque basado en las capacidades, puede crear un entorno para implementar, operar y administrar sus cargas de trabajo. También puede mejorar las capacidades para ampliar su entorno a medida que evolucionen sus requisitos e implemente cargas de trabajo adicionales en la nube. Para obtener más información sobre las 30 capacidades de AWS, consulte Capacidades. En esta guía, se incluyen las prácticas recomendadas para implementar las capacidades iniciales en el orden previsto.

Puede adoptar e implementar capacidades de acuerdo con sus necesidades operativas y de gobernanza. A medida que sus requisitos empresariales vayan madurando, el enfoque basado en capacidades se puede utilizar como mecanismo para comprobar que su entorno de nube está preparado para soportar sus cargas de trabajo y escalar según sea necesario. Este enfoque le permite establecer con confianza su entorno en la nube para sus desarrolladores y su empresa.

Administración de identidades y control de acceso para la transición a una arquitectura de varias cuentas

El primer paso al realizar la transición a una arquitectura de varias cuentas consiste en configurar la nueva estructura de cuentas dentro de una organización. A continuación, puede agregar usuarios y configurar el acceso a las cuentas. En esta sección, se describen los enfoques para administrar el acceso humano a varias Cuentas de AWS.

Esta guía contiene las siguientes tareas:

- Configuración de una organización
- Crear una zona de aterrizaje
- Agregar unidades organizativas
- Agregar usuarios iniciales
- Administrar las cuentas miembro

Configuración de una organización

Si tiene varias Cuentas de AWS, puedes administrar esas cuentas de forma lógica a través de una organización en AWS Organizations. Una cuenta en AWS Organizations es una Cuenta de AWS estándar que contiene sus recursos de AWS y las identidades que pueden acceder a esos recursos. Una organización es una entidad que consolida sus Cuentas de AWS para que pueda administrarlas como una única unidad.

Si utiliza una cuenta para crear una organización, esa cuenta se convierte en cuenta de administración (también conocida como cuenta de pagador o cuenta raíz) para la organización. Una organización solo puede tener una cuenta de administración. Cuando agrega más Cuentas de AWS a la organización, se convierten en cuentas miembro.

> **Note**
>
> Cada Cuenta de AWS también tiene una identidad única llamada usuario raíz. Puede iniciar sesión como usuario raíz mediante la dirección de correo electrónico y contraseña que usó al crear la cuenta. Sin embargo, se recomienda encarecidamente no utilizar el usuario raíz

para las tareas cotidianas, ni siquiera para las tareas administrativas. Para obtener más información, consulte Usuario raíz de Cuenta de AWS.

Las cuentas se organizan en una estructura de árbol jerárquica que consiste en la organización raíz, las unidades organizativas (OU) y las cuentas miembro. La raíz es el contenedor principal de todas las cuentas de su organización. Una unidad organizativa (OU) es un contenedor para cuentas dentro de la raíz. Una OU puede contener otras OU o cuentas miembro. Una unidad organizativa puede tener un solo contenedor principal y cada cuenta puede ser miembro de una sola unidad organizativa. Para obtener más información, consulte Terminología y conceptos (documentación de AWS Organizations).

Una política de control de servicios (SCP) especifica los servicios y las acciones que pueden usar los usuarios y los roles. Las SCP son similares a las políticas de permisos de AWS Identity and Access Management (IAM), con la salvedad de que no conceden permisos. En cambio, las SCP definen los permisos máximos. Al adjuntar una política a uno de los nodos de la jerarquía, se aplica a todas las unidades organizativas y cuentas de ese nodo. Por ejemplo, si se aplica una política a la raíz, se aplica a todas las OU y cuentas de la organización, y si se aplica una política a una OU, se aplica solo a las OU y cuentas de la organización en la OU destino.

Puede utilizar la consola de AWS Organizations para ver y administrar de forma centralizada todas las cuentas de una organización. Una de las ventajas de utilizar una organización es que puede recibir una factura unificada que muestra todos los cargos asociados a las cuentas miembro y de administración. Para obtener más información, consulte Factura unificada (documentación de AWS Organizations).

Prácticas recomendadas

- No utilice una Cuenta de AWS existente para crear una organización. Comience con una cuenta nueva, que pasará a ser la cuenta de administración de la organización. Las operaciones privilegiadas se pueden realizar dentro de la cuenta de administración de una organización y las SCP no se aplican a dicha cuenta. Por eso, debe limitar los recursos y datos de la nube que contenga la cuenta de administración únicamente a los que deben administrarse en esta cuenta.
- Limite el acceso a la cuenta de administración solo a aquellas personas que necesiten aprovisionar nuevas Cuentas de AWS y administrar la organización.
- Use las SCP para definir los permisos máximos para la raíz, las unidades organizativas y las cuentas miembros. Las SCP no se pueden aplicar directamente a la cuenta de administración.

- Siga las Prácticas recomendadas de AWS Organizations (documentación de AWS Organizations).

Crear una zona de aterrizaje

Una zona de aterrizaje es un entorno de AWS de varias cuentas y de buena arquitectura que será el punto de partida desde el que podrá implementar cargas de trabajo y aplicaciones. Ofrece una base de referencia para empezar con la arquitectura de varias cuentas, la administración de identidades y accesos, la gobernanza, la seguridad de los datos, el diseño de redes y el registro. AWS Control Tower es un servicio que simplifica el mantenimiento y la gobernanza de un entorno de varias cuentas, ya que brinda barreras de protección automatizadas. Por lo general, se aprovisiona una sola zona de aterrizaje de AWS Control Tower que administra su entorno en todas las Regiones de AWS. AWS Control Tower funciona orquestando otros Servicios de AWS dentro de su cuenta. Para obtener más información, consulte ¿Qué sucede cuando se configura una zona de aterrizaje? (documentación de AWS Control Tower).

Cuando configura una zona de aterrizaje con AWS Control Tower, puede identificar tres cuentas compartidas: la cuenta de administración, la cuenta de archivo de registros y la cuenta de auditoría. Para obtener más información, consulte ¿Qué son las cuentas compartidas? (documentación de AWS Control Tower). Para la cuenta de administración, debe usar una cuenta existente que no aloje ninguna carga de trabajo para configurar la zona de aterrizaje. Para el archivo de registros y las cuentas de auditoría, puede optar por reutilizar las Cuentas de AWS existentes o AWS Control Tower puede crearlas por usted.

Para obtener instrucciones sobre cómo configurar su zona de aterrizaje de AWS Control Tower, consulte Introducción (documentación de AWS Control Tower).

Prácticas recomendadas

- Siga las prácticas recomendadas en Principios de diseño para su estrategia de varias cuentas (documento técnico de AWS).
- Siga las Prácticas recomendadas para administradores de AWS Control Tower (documentación de AWS Control Tower).
- Cree su zona de aterrizaje en Región de AWS que alojará la mayoría de sus cargas de trabajo.

> **Important**
>
> Si decide cambiar esta región después de implementar su zona de aterrizaje, necesitará la ayuda de AWS Support y deberá retirar la zona de aterrizaje. No se recomienda esta práctica.

- Al determinar qué regiones regirá AWS Control Tower, seleccione solo las regiones en las que espera implementar cargas de trabajo de forma inmediata. Puede cambiar estas regiones o agregar otras más adelante. Si AWS Control Tower gobierna una región, implementará sus barreras de protección de detección en esa región como Reglas de AWS Config.
- Después de determinar qué regiones gobernará AWS Control Tower, niegue el acceso a todas las regiones no gobernadas. De esta forma, se garantiza que sus cargas de trabajo y los desarrolladores solo puedan utilizar las Regiones de AWS aprobadas. Esto se implementa como una política de control de servicio (SCP) en la organización. Para obtener más información, consulte Configure the Región de AWS deny control (documentación de AWS Control Tower).
- Al configurar su zona de aterrizaje en AWS Control Tower, se recomienda que cambie el nombre de las siguientes unidades organizativas y cuentas:
  - Se recomienda que cambie el nombre de la unidad organizativa Seguridad a Security_Prod para indicar que esta OU se utilizará para las Cuentas de AWS de producción relacionadas con la seguridad.
  - Le recomendamos que permita que AWS Control Tower cree una unidad organizativa adicional y luego le cambie el nombre de Entorno aislado a Cargas de trabajo. En la siguiente sección, se crean unidades organizativas adicionales dentro de la unidad organizativa Cargas de trabajo, que se utilizan para organizar las Cuentas de AWS.
  - Se recomienda cambiar el nombre de la Cuenta de AWS de registro centralizado de Archivo de registros a log-archive-prod.
  - Se recomienda cambiar el nombre de la cuenta de auditoría Auditoría a security-tooling-prod.
- Para ayudar a prevenir el fraude, AWS requiere que las Cuentas de AWS tengan un historial de uso antes de que puedan agregarse a una zona de aterrizaje de AWS Control Tower. Si utiliza una nueva Cuenta de AWS sin ningún historial de uso, en la nueva cuenta puede lanzar una instancia de Amazon Elastic Compute Cloud (Amazon EC2) que no se encuentre en el nivel gratuito de AWS. Deje que la instancia se ejecute durante unos minutos y, a continuación, ciérrela.

Agregar unidades organizativas

Establecer la estructura organizativa adecuada es fundamental para configurar un entorno de varias cuentas. Dado que utiliza políticas de control de servicio (SCP) para definir los permisos máximos para una OU y las cuentas que contiene, la estructura de su organización debe ser lógica desde el punto de vista de la administración, los permisos y los informes financieros. Para obtener más información sobre la estructura de una organización, incluidas las unidades organizativas (OU), consulte Terminología y conceptos (documentación de AWS Organizations).

En esta sección, puede personalizar la zona de aterrizaje mediante la creación de unidades organizativas anidadas que lo ayudan a segmentar y estructurar sus entornos, como los de producción y los de no producción. Estas prácticas recomendadas están diseñadas para segmentar la zona de aterrizaje y así separar los recursos de producción y los que no son de producción y, también, para separar la infraestructura de las cargas de trabajo.

Para obtener más información acerca de las unidades organizativas, consulte Administración de unidades organizativas (documentación de AWS Organizations).

Prácticas recomendadas

- Dentro de la unidad organizativa Cargas de trabajo que creó en Crear una zona de aterrizaje, cree las siguientes unidades organizativas anidadas:
  - Prod: utilice esta OU para las Cuentas de AWS que almacenan y acceden a los datos de producción, incluidos los datos de los clientes.
  - NonProd: utilice esta OU para las Cuentas de AWS que almacenan datos que no son de producción, como entornos de desarrollo, montaje o pruebas.

En la raíz de la organización, cree una OU Infrastructure_Prod. Utilice esta OU para alojar una cuenta de red centralizada.

Agregar usuarios iniciales

Existen dos formas de conceder a las personas el acceso a las Cuentas de AWS:

- Identidades de IAM, como usuarios, grupos y roles
- Federación de identidades, por ejemplo, mediante el uso de AWS IAM Identity Center

En las empresas más pequeñas y en los entornos de una única cuenta, es habitual que los administradores creen un usuario de IAM cuando una nueva persona se incorpora a la empresa. Las credenciales de clave de acceso y clave secreta asociadas a un usuario de IAM se conocen como credenciales de larga duración porque no caducan. Sin embargo, esta no es una práctica de seguridad recomendada, ya que si un atacante pone en peligro esas credenciales, entonces se deberá que generar un nuevo conjunto de credenciales para el usuario. Otro enfoque para acceder a las Cuentas de AWS es a través de los roles de IAM. También puede usar AWS Security Token Service (AWS STS) para solicitar temporalmente credenciales de corto plazo, que caducan tras un periodo configurable.

Puede administrar el acceso de las personas a sus Cuentas de AWS mediante IAM Identity Center. Puede crear cuentas de usuario individuales para cada uno de sus empleados o contratistas, que pueden administrar sus propias contraseñas y soluciones de autenticación multifactor (MFA), y puede agruparlas para administrar el acceso. Al configurar la MFA, puede usar tokens de software, como aplicaciones de autenticación, o puede usar tokens de equipo, como los dispositivos YubiKey.

IAM Identity Center también admite la federación de proveedores de identidades externos (IdP), como Okta, JumpCloud y Ping Identity. Para obtener más información, consulte Proveedores de identidades compatibles (documentación de IAM Identity Center). Al federarse con un IdP externo, puede administrar la autenticación de los usuarios en todas las aplicaciones y luego utilizar IAM Identity Center para autorizar el acceso a determinadas Cuentas de AWS.

Prácticas recomendadas

- Siga las prácticas recomendadas de seguridad (documentación de IAM) para configurar el acceso de los usuarios.
- Administre el acceso a las cuentas por grupos en lugar de por usuarios individuales. En IAM Identity Center, cree nuevos grupos que representen cada una de sus funciones empresariales. Por ejemplo, puede crear grupos para ingeniería, finanzas, ventas y administración de productos.
- A veces, los grupos se definen separando a aquellos que necesitan acceso a todas las Cuentas de AWS (a menudo acceso de solo lectura) y aquellos que necesitan acceso a una única Cuenta de AWS. Se recomienda la siguiente convención de nomenclatura para grupos para que se pueda identificar con facilidad las Cuenta de AWS y permisos asociados al grupo.

  `<prefix>-<account name>-<permission set>`
- Por ejemplo, para el grupo `AWS-A-dev-nonprod-DeveloperAccess`, `AWS-A` es un prefijo que indica el acceso a una única cuenta, `dev-nonprod` es el nombre de la cuenta y `DeveloperAccess` es el conjunto de permisos asignado al grupo. Para el grupo `AWS-O-`

`BillingAccess`, el prefijo `AWS-0` indica el acceso a toda la organización y `BillingAccess` indica el conjunto de permisos para el grupo. En este ejemplo, dado que el grupo tiene acceso a toda la organización, el nombre del grupo no representa el nombre de una cuenta.

- Si utiliza IAM Identity Center con un IdP externo basado en SAML y desea requerir MFA, puede usar el control de acceso basado en atributos (ABAC) para pasar el método de autenticación del IdP a IAM Identity Center. Los atributos se envían mediante las aserciones de SAML. Para obtener más información, consulte Habilitar y configurar los atributos para el control de acceso (documentación de IAM Identity Center).

  Muchos IdP, como Microsoft Azure Active Directory y Okta, pueden usar la reclamación de la referencia del método de autenticación (`amr`) dentro de una aserción de SAML para pasar el estado de MFA del usuario a IAM Identity Center. La reclamación utilizada para afirmar el estado de MFA y su formato varían según el IdP. Para obtener más información, consulte la documentación de su IdP.

  En IAM Identity Center, puede crear políticas de conjunto de permisos para determinar quién puede acceder a sus recursos de AWS. Cuando habilita ABAC y especifica atributos, IAM Identity Center transfiere los valores de atributo del usuario autenticado a IAM para utilizarlos en la evaluación de políticas. Para obtener más información, consulte Crear políticas de permisos para ABAC (documentación de IAM Identity Center). Como se muestra en el siguiente ejemplo, se utiliza la clave de condición de `aws:PrincipalTag` para crear una regla de control de acceso para la MFA.

```
"Condition": {
  "StringLike": { "aws:PrincipalTag/amr": "mfa" }
}
```

Administrar las cuentas miembro

En esta sección, usted invita a su cuenta preexistente a la organización y comienza a crear nuevas cuentas en la organización. Una parte importante de este proceso consiste en definir los criterios que se utilizan para determinar si es necesario aprovisionar una cuenta nueva.

Esta guía contiene las siguientes tareas:

- Invitación a su cuenta preexistente
- Personalizar la configuración de VPC en AWS Control Tower

- Configuración de los criterios de alcance

Invitación a su cuenta preexistente

Dentro de AWS Organizations, puede invitar a la cuenta preexistente de su empresa a su nueva organización. Solo la cuenta de administración de la organización puede invitar a otras cuentas a unirse. En el momento en que el administrador de la cuenta miembro acepta, la cuenta se une inmediatamente a la organización y la cuenta de administración de la organización se hace responsable de todos los cargos acumulados por la nueva cuenta miembro. Para obtener más información, consulte Invitar a una Cuenta de AWS para unirse a su organización y Aceptar o rechazar una invitación de una organización (documentación de AWS Organizations).

> **Note**
>
> Puede invitar a una cuenta a unirse a una organización solo si esa cuenta no está actualmente en otra organización. Si la cuenta es miembro de una organización existente, debe eliminarla de la organización. Si la cuenta es la cuenta de administración de otra organización que se creó por error, debe eliminar la organización.

> **Important**
>
> Si necesita acceder a cualquier información histórica sobre costos o uso de su cuenta preexistente, puede usar AWS Cost and Usage Report para exportar esa información a un bucket de Amazon Simple Storage Service (Amazon S3). Haga esto antes de aceptar la invitación para unirse a la organización. Cuando una cuenta se une a una organización, se pierde el acceso a estos datos históricos de la cuenta. Para obtener más información, consulte Configuración de un bucket de Amazon S3 para los informes de costo y uso (documentación de AWS Cost and Usage Report).

Prácticas recomendadas

- Se recomienda que agregue su cuenta preexistente, que probablemente contenga cargas de trabajo de producción, a la unidad organizativa Cargas de trabajo > Prod que creó en Agregar unidades organizativas .

- De forma predeterminada, la cuenta de administración de la organización no tiene acceso administrativo a las cuentas miembro que están invitadas a la organización. Si desea que la cuenta de administración tenga control administrativo, debe crear el rol de IAM OrganizationAccountAccessRole en la cuenta miembro y conceder permiso a la cuenta de administración para que asuma el rol. Para obtener más información, consulte Crear el rol OrganizationAccountAccessRole en una cuenta miembro invitada (documentación AWS Organizations).
- Para la cuenta preexistente que ha invitado a la organización, consulte Prácticas recomendadas para cuentas miembro (documentación de AWS Organizations) y confirme que la cuenta sigue estas recomendaciones.

Personalizar la configuración de VPC en AWS Control Tower

Se recomienda que se aprovisione nuevas Cuentas de AWS a través de Fábrica de cuentas en AWS Control Tower. Al usar Fábrica de cuentas, puede usar la integración de AWS Control Tower con Amazon EventBridge para aprovisionar recursos en Cuentas de AWS nuevas tan pronto como se cree la cuenta.

Cuando configura una nueva Cuenta de AWS, se aprovisiona automáticamente una nube privada virtual (VPC) predeterminada. Sin embargo, cuando configura una cuenta nueva a través de Fábrica de cuentas, AWS Control Tower aprovisiona automáticamente una VPC adicional. Para obtener más información, consulte Descripción general de AWS Control Tower y VPC (documentación de AWS Control Tower). Esto significa que, por defecto, AWS Control Tower brinda dos VPC predeterminadas en cada cuenta nueva.

Es habitual que las empresas deseen tener más control sobre los VPC de sus cuentas. Muchas prefieren utilizar otros servicios, como AWS CloudFormation, Hashicorp Terraform o Pulumi, para configurar y administrar sus VPC. Debe personalizar la configuración de Fábrica de cuentas para evitar la creación de la VPC adicional aprovisionada por AWS Control Tower. Para obtener instrucciones, consulte Configuración de ajustes de Amazon VPC (documentación de AWS Control Tower) y aplique la siguiente configuración:

1. Deshabilite la opción Subred accesible a Internet.
2. En Número de subredes privadas, elija 0.
3. En Regiones para la creación de VPC, borre todas las regiones.
4. En Zonas de disponibilidad, elija 3.

Prácticas recomendadas

- Elimine la VPC predeterminada que se aprovisiona automáticamente en cada cuenta nueva. Esto impide que los usuarios lancen instancias de EC2 públicas en la cuenta sin crear explícitamente una VPC dedicada. Para obtener más información, consulte Eliminar las subredes predeterminadas y la VPC predeterminada (documentación de Amazon Virtual Private Cloud). También puede configurar Fábrica de cuentas de AWS Control Tower para Terraform (AFT) para eliminar automáticamente la VPC predeterminada en las cuentas recién creadas.
- Aprovisione una nueva Cuenta de AWS llamada dev-nonprod en la unidad organizativa Cargas de trabajo > NonProd. Utilice esta cuenta para su entorno de desarrollo. Para obtener instrucciones, consulte Aprovisionamiento de las cuentas de Fábrica de cuentas con AWS Service Catalog (documentación AWS Control Tower).

Configuración de los criterios de alcance

Debe seleccionar los criterios que utilizará su empresa a la hora de decidir si aprovisiona una nueva Cuenta de AWS. Puede decidir aprovisionar cuentas para cada unidad de negocio o aprovisionar cuentas en función del entorno, como la producción, las pruebas o el control de calidad. Cada empresa tiene sus propios requisitos en cuanto al tamaño de sus Cuentas de AWS. Por lo general, usted evalúa los tres factores siguientes al decidir el tamaño de sus cuentas:

- Equilibrio de las cuotas de servicio: las cuotas de servicio son los valores máximos para la cantidad de recursos, acciones y elementos para cada Servicio de AWS dentro de una Cuenta de AWS. Si muchas cargas de trabajo comparten la misma cuenta y una carga de trabajo consume la mayor parte o la totalidad de una cuota de servicio, eso podría afectar de manera negativa a otra carga de trabajo de la misma cuenta. Si es así, es posible que tenga que separar esas cargas de trabajo en cuentas diferentes. Para obtener más información, consulte Cuotas de Servicio de AWS (Referencia general de AWS).
- Informes de costos: aislar las cargas de trabajo en cuentas separadas le permite ver los costos a nivel de cuenta en los informes de costos y uso. Cuando utiliza la misma cuenta para varias cargas de trabajo, puede usar etiquetas para que lo ayuden a administrar e identificar los recursos. Para obtener más información acerca del etiquetado, consulte Etiquetado de recursos de AWS (Referencia general de AWS).
- Control de acceso: cuando las cargas de trabajo comparten una cuenta, debe tener en cuenta cómo va a configurar las políticas de IAM para limitar el acceso a los recursos de la cuenta, de modo que los usuarios no tengan acceso a las cargas de trabajo que no necesitan. Como

alternativa, puede utilizar varias cuentas y conjuntos de permisos en IAM Identity Center para administrar el acceso a las cuentas individuales.

Prácticas recomendadas

- Siga las prácticas recomendadas en estrategia de varias cuentas de AWS para su zona de aterrizaje de AWS Control Tower (documentación de AWS Control Tower).
- Establezca una estrategia de etiquetado eficaz que lo ayude a identificar y administrar los recursos de AWS. Utilice etiquetas para clasificar los recursos según su finalidad, unidad de negocio, entorno u otro criterio. Para obtener más información, consulte Prácticas recomendadas para el etiquetado (documentación de Referencia general de AWS).
- No sobrecargue una cuenta con demasiadas cargas de trabajo. Si la demanda de la carga de trabajo supera una cuota de servicio, esto puede provocar problemas de rendimiento. Puede separar las cargas de trabajo competitivas en diferentes Cuentas de AWS o puede solicitar un aumento de la cuota de servicio. Para obtener más información, consulte Solicitar un aumento de cuota (documentación de Service Quotas).

Administración de permisos y acceso para una arquitectura de varias cuentas

Esta sección consta de los siguientes temas:

- Consideraciones culturales de ingeniería
- Creación de conjuntos de permisos
- Creación de un límite de permisos
- Administración de los permisos de los individuos

Consideraciones culturales de ingeniería

Uno de los pilares del Marco de AWS Well-Architected es la excelencia operativa. Los equipos deben entender el modelo operativo y su papel en el logro de los resultados de su negocio. Los equipos pueden centrarse en alcanzar los objetivos compartidos cuando comprenden sus responsabilidades, son capaces de asumirlas y saben cómo se toman las decisiones.

Con empresas en fase inicial que se están desarrollando rápidamente, todos los miembros del equipo desempeñan varios roles. No es raro que estos usuarios tengan un acceso altamente privilegiado a toda la Cuenta de AWS. A medida que las empresas crecen, a menudo quieren seguir el principio de privilegio mínimo y solo conceden los permisos necesarios para que el usuario pueda realizar su trabajo. Para ayudarlo a limitar el alcance, puede usar AWS Identity and Access Management Access Analyzer para ver qué permisos utiliza realmente un usuario o un rol de IAM, lo que le permite eliminar cualquier exceso de permisos.

Decidir quién en su empresa tiene permisos para crear roles de IAM puede resultar difícil. Suele ser un vector para escalar privilegios. La escalada de privilegios se produce cuando un usuario puede ampliar sus propios permisos o su alcance de acceso. Por ejemplo, si un usuario tiene permisos limitados, pero puede crear nuevos roles de IAM, ese usuario podría escalar sus privilegios al crear y asumir un nuevo rol de IAM que tenga aplicada la política administrada `AdministratorAccess`.

Algunas empresas limitan el aprovisionamiento de roles de IAM a un equipo centralizado de individuos de confianza. La desventaja de este enfoque es que el equipo puede convertirse rápidamente en un cuello de botella, ya que casi todos los Servicios de AWS requieren un rol de IAM para funcionar. Como alternativa, puede utilizar límites de permisos para delegar el acceso a IAM

únicamente a los usuarios que desarrollen, prueben, lancen y administren su infraestructura de nube. Para ver ejemplos de políticas, consulte Ejemplos de límites de permisos(GitHub).

Los equipos de operaciones de desarrollo (DevOps), también conocidos como equipos de plataforma, a menudo, necesitan equilibrar las capacidades de autoservicio de varios equipos de desarrollo interno con la estabilidad operativa de las aplicaciones. Fomentar una cultura de ingeniería que abarque la autonomía, el dominio y el propósito en el lugar de trabajo puede ayudar a motivar a los equipos. Los ingenieros quieren hacer su trabajo de manera autodirigida, sin depender de que otros hagan las cosas por ellos. Si los equipos de DevOps pueden implementar soluciones de autoservicio, esto también reduce la cantidad de tiempo que otros dependen de ellos para hacer las cosas.

Creación de conjuntos de permisos

Puede administrar el acceso a la Cuenta de AWS mediante conjuntos de permisos en AWS IAM Identity Center. Un conjunto de permisos es una plantilla que lo ayuda a implementar una o más políticas de IAM en varias Cuentas de AWS. Al asignar un conjunto de permisos para configurar una Cuenta de AWS, IAM Identity Center crea un rol de IAM y asocia las políticas de IAM a ese rol. Para obtener más información, consulte Crear y administrar conjuntos de permisos (documentación de IAM Identity Center).

AWS recomienda crear conjuntos de permisos que se correspondan con las distintas personas de su empresa.

Por ejemplo, puede crear los siguientes conjuntos de permisos:

- Conjunto de permisos de facturación
- Conjunto de permisos de desarrollador
- Conjunto de permisos de producción

Los siguientes conjuntos de permisos son fragmentos de una plantilla de AWS CloudFormation. Debería usar este código como punto de partida y personalizarlo para su negocio. Para obtener más información acerca de las plantillas de CloudFormation, consulte Más información sobre los aspectos básicos de las plantillas (documentación de CloudFormation).

Conjunto de permisos de facturación

El equipo de finanzas usa BillingAccessPermissionSet para ver el panel de control de la consola de AWS Billing y AWS Cost Explorer en cada cuenta.

```
BillingAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to Billing and Cost Explorer
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/Billing"
    Name: BillingAccess
    SessionDuration: PT8H
    RelayStateType: https://console.aws.amazon.com/billing/home
```

Conjunto de permisos de desarrollador

El equipo de ingeniería utiliza DeveloperAccessPermissionSet para acceder a cuentas que no son de producción.

```
DeveloperAccessPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to provision resources through CloudFormation
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:ContinueUpdateRollback",
              "cloudformation:CreateChangeSet",
              "cloudformation:CreateStack",
              "cloudformation:DeleteStack",
```

```
              "cloudformation:RollbackStack",
              "cloudformation:UpdateStack"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app/*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              },
              "Null": {
                "cloudformation:ImportResourceTypes": true
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": [
              "cloudformation:CancelUpdateStack",
              "cloudformation:DeleteChangeSet",
              "cloudformation:DetectStackDrift",
              "cloudformation:DetectStackResourceDrift",
              "cloudformation:ExecuteChangeSet",
              "cloudformation:TagResource",
              "cloudformation:UntagResource",
              "cloudformation:UpdateTerminationProtection"
            ],
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app/*"
          },
          {
           "Effect": "Allow",
            "Action": [
              "cloudformation:CreateUploadBucket",
              "cloudformation:ValidateTemplate",
              "cloudformation:EstimateTemplateCost"
            ],
            "Resource": "*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSServiceCatalogEndUserFullAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSProtonDeveloperAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
```

```
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/ReadOnlyAccess"
    Name: DeveloperAccess
    SessionDuration: PT8H
```

Conjunto de permisos de producción

El equipo de ingeniería utiliza ProductionPermissionSet para acceder a las cuentas de producción. Este conjunto de permisos tiene acceso limitado y de solo lectura.

```
ProductionPermissionSet:
  Type: "AWS::SSO::PermissionSet"
  Properties:
    Description: Access to production accounts
    InlinePolicy: !Sub |-
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": "arn:${AWS::Partition}:iam::*:role/CloudFormationRole",
            "Condition": {
              "StringEquals": {
                "aws:ResourceAccount": "${!aws:PrincipalAccount}",
                "iam:PassedToService": "cloudformation.${AWS::URLSuffix}"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:ContinueUpdateRollback",
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app/*",
            "Condition": {
              "ArnLike": {
                "cloudformation:RoleArn": "arn:${AWS::Partition}:iam::${!
aws:PrincipalAccount}:role/CloudFormationRole"
              }
            }
          },
          {
            "Effect": "Allow",
            "Action": "cloudformation:CancelUpdateStack",
```

```
            "Resource": "arn:${AWS::Partition}:cloudformation:*:*:stack/app/*"
          }
        ]
      }
    InstanceArn: !Sub "arn:${AWS::Partition}:sso:::instance/ssoins-instanceId"
    ManagedPolicies:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSBillingReadOnlyAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AWSSupportAccess"
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/job-function/ViewOnlyAccess"
    Name: ProductionAccess
    SessionDuration: PT2H
```

Creación de un límite de permisos

Después de implementar los conjuntos de permisos, debe establecer un límite de permisos. Este límite de permisos es un mecanismo para delegar el acceso a IAM únicamente a los usuarios que están desarrollando, probando, lanzando y administrando su infraestructura de nube. Esos usuarios solo pueden realizar las acciones permitidas por la política y el límite de permisos.

Puede definir el límite de permisos en una plantilla de AWS CloudFormation y luego usar CloudFormation StackSets para implementar la plantilla en varias cuentas. Esto lo ayuda a establecer y mantener políticas estandarizadas en toda la organización con una sola operación. Para obtener más información, consulte Trabajo con AWS CloudFormation StackSets (documentación de CloudFormation).

En la siguiente plantilla de CloudFormation, se brinda un rol de IAM y crea una política de IAM que actúa como límite de permisos. Con un conjunto de pilas, puede implementar esta plantilla en todas las cuentas miembro de su organización.

```
CloudFormationRole:
  Type: "AWS::IAM::Role"
  Properties:
    AssumeRolePolicyDocument:
      Version: "2012-10-17"
      Statement:
        Effect: Allow
        Principal:
          Service: !Sub "cloudformation.${AWS::URLSuffix}"
        Action: "sts:AssumeRole"
        Condition:
          StringEquals:
```

```
            "aws:SourceAccount": !Ref "AWS::AccountId"
    Description: !Sub "DO NOT DELETE - Used by CloudFormation. Created by
 CloudFormation ${AWS::StackId}"
    ManagedPolicyArns:
      - !Sub "arn:${AWS::Partition}:iam::aws:policy/AdministratorAccess"
    PermissionsBoundary: !Ref DeveloperBoundary
    RoleName: CloudFormationRole

DeveloperBoundary:
  Type: "AWS::IAM::ManagedPolicy"
  Properties:
    Description: Permission boundary for developers
    ManagedPolicyName: PermissionsBoundary
    PolicyDocument:
      Version: "2012-10-17"
      Statement:
        - Sid: AllowModifyIamRolesWithBoundary
          Effect: Allow
          Action:
            - "iam:AttachRolePolicy"
            - "iam:CreateRole"
            - "iam:DeleteRolePolicy"
            - "iam:DetachRolePolicy"
            - "iam:PutRolePermissionsBoundary"
            - "iam:PutRolePolicy"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
          Condition:
            ArnEquals:
              "iam:PermissionsBoundary": !Sub "arn:${AWS::Partition}:iam::
${AWS::AccountId}:policy/PermissionsBoundary"
        - Sid: AllowModifyIamRoles
          Effect: Allow
          Action:
            - "iam:DeleteRole"
            - "iam:TagRole"
            - "iam:UntagRole"
            - "iam:UpdateAssumeRolePolicy"
            - "iam:UpdateRole"
            - "iam:UpdateRoleDescription"
          Resource: !Sub "arn:${AWS::Partition}:iam::${AWS::AccountId}:role/app/*"
        - Sid: OverlyPermissiveAllowedServices
          Effect: Allow
          Action:
            - "lambda:*"
```

```
            - "apigateway:*"
            - "events:*"
            - "s3:*"
            - "logs:*"
          Resource: "*"
```

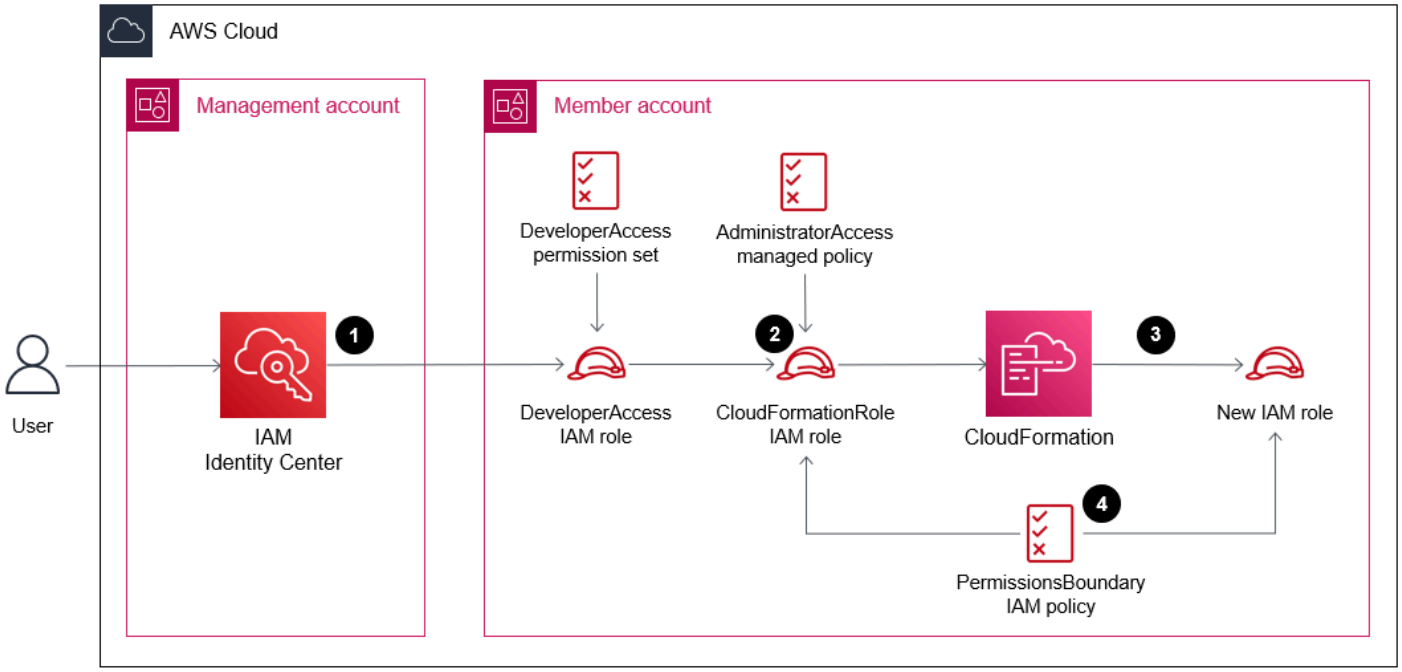
El rol CloudFormationRole, la política PermissionsBoundary y el conjunto de permisos DeveloperAccess funcionan en conjunto para conceder los siguientes permisos:

- Los usuarios tienen acceso de solo lectura a la mayoría de los Servicios de AWS, a través de la política administrada de AWS ReadOnlyAccess.
- Los usuarios tienen acceso a los casos de soporte abiertos a través de la política administrada de AWS AWSSupportAccess.
- Los usuarios tienen acceso de solo lectura al panel de control de la consola de AWS Billing, a través de la política AWSBillingReadOnlyAccess administrada por AWS.
- Los usuarios pueden aprovisionar nuevos entornos desde AWS Proton, a través de la política administrada de AWS AWSProtonDeveloperAccess.
- Los usuarios pueden aprovisionar productos desde Service Catalog, a través de la política administrada de AWS AWSServiceCatalogEndUserFullAccess.
- Los usuarios pueden validar y estimar el costo de cualquier plantilla de CloudFormation mediante la política en línea.
- Mediante el uso del rol de IAM CloudFormationRole, los usuarios pueden crear, actualizar o eliminar cualquier pila de CloudFormation que comience con app/.
- Los usuarios pueden usar CloudFormation para crear, actualizar o eliminar roles de IAM que comiencen con app/. La política de IAM PermissionsBoundary impide que los usuarios escalen sus privilegios.
- Los usuarios pueden aprovisionar recursos de AWS Lambda, Amazon EventBridge, Amazon CloudWatch, Amazon Simple Storage Service (Amazon S3) y Amazon API Gateway únicamente mediante CloudFormation.

En la siguiente imagen, se muestra cómo un usuario autorizado, como un desarrollador, puede crear un nuevo rol de IAM en una cuenta miembro mediante los conjuntos de permisos, los roles de IAM y los límites de permisos que se describen en esta guía:

1. El usuario se autentica en IAM Identity Center y asume el rol de IAM DeveloperAccess.

2. El usuario inicia la acción `cloudformation:CreateStack` y asume el rol de IAM CloudFormationRole.
3. El usuario inicia la acción `iam:CreateRole` y usa CloudFormation para crear un nuevo rol de IAM.
4. La política de IAM PermissionsBoundary se aplica al nuevo rol de IAM.



El rol CloudFormationRole tiene la política AdministratorAccess administrada adjunta, pero debido a la política de IAM PermissionsBoundary, los permisos eficaces del rol CloudFormationRole pasan a ser iguales a la política PermissionsBoundary. La política PermissionsBoundary hace referencia a sí misma cuando permite la acción `iam:CreateRole`, que garantiza que los roles solo se puedan crear si se aplica el límite de permisos.

Administración de los permisos de los individuos

Mediante el uso de conjuntos de permisos, el límite de permisos y el rol de IAM CloudFormationRole, puede limitar la cantidad de permisos que necesita asignar directamente a las entidades principales individuales. Esto lo ayuda a administrar el acceso a medida que la empresa crece y a aplicar las prácticas de seguridad recomendadas de conceder privilegios mínimos.

También puedes usar roles vinculados a servicio, que otorgan permisos a un servicio de AWS para aprovisionar recursos en su nombre. En lugar de conceder permisos a la entidad principal de IAM

(usuario, grupo de usuarios o rol), puede conceder los permisos al servicio. Por ejemplo, los roles vinculados a servicio para AWS Proton y AWS Service Catalog le permiten aprovisionar sus propias plantillas, recursos y entornos sin asignar permisos a la entidad principal de IAM. Para obtener más información, consulte Servicios de AWS que funcionan con IAM y Uso de roles vinculados a servicio (documentación de IAM).

Otra práctica recomendada es limitar la cantidad de acceso que tienen los individuos a AWS Management Console. Al limitar el acceso a la consola, puede requerir que los individuos aprovisionen recursos mediante tecnologías de infraestructura como código (IaC), como AWS CloudFormation, HashiCorp Terraform o Pulumi. Administrar la infraestructura a través de IaC permite realizar un seguimiento de los cambios en los recursos a lo largo del tiempo e introducir mecanismos para aprobar los cambios, como las solicitudes de cambios de GitHub.

Conectividad de red para una arquitectura de varias cuentas

Conexión de las VPC

Muchas empresas utilizan interconexiones de VPC en Amazon Virtual Private Cloud (Amazon VPC) para conectar las VPC de desarrollo y producción. Con una conexión de emparejamiento de VPC, puede enrutar el tráfico entre dos VPC mediante el uso de dirección IP privada. Las VPC conectadas pueden estar en diferentes Cuentas de AWS y en diferentes Regiones de AWS. Para obtener más información, consulte ¿Qué es una interconexión de VPC? (documentación de Amazon VPC). A medida que las empresas crecen y aumenta el número de VPC, mantener conexiones de emparejamiento entre todas las VPC puede convertirse en una carga de mantenimiento. También puede estar limitado por la cantidad máxima de conexiones de emparejamiento de VPC por VPC. Para obtener más información, consulte Cuota de conexiones de emparejamiento de VPC (documentación de Amazon VPC).

Si tiene varios entornos de desarrollo, prueba y puesta en escena que alojan datos no relacionados con la producción en varios entornos Cuentas de AWS, tal vez desee proporcionar conectividad de red entre todas esas VPC, pero no permitir el acceso a los entornos de producción. Puede usar AWS Transit Gateway para conectar varias VPC en varias cuentas. Puede separar las tablas de enrutamiento para evitar que las VPC de desarrollo se comuniquen con las VPC de producción a través de la puerta de enlace de tránsito, que actúa como enrutador centralizado. Para obtener más información, consulte Enrutador centralizado (documentación de Transit Gateway).

Transit Gateway también admite la interconexión con otras puertas de enlace de tránsito, incluidas las de diferentes Cuentas de AWS o Regiones de AWS. Como Transit Gateway es un servicio totalmente administrado y de alta disponibilidad, solo necesita aprovisionar una puerta de enlace de tránsito para cada región.

Para obtener más información y arquitecturas de red detalladas, consulte Creación de una infraestructura de AWS red multiVPC escalable y segura (AWS documento técnico).

Conexión de aplicaciones

Si necesita establecer la comunicación entre aplicaciones diferentes Cuentas de AWS en el mismo entorno (como el de producción), puede utilizar una de las siguientes opciones:

- La interconexión de VPC o AWS Transit Gateway pueden brindar conectividad a nivel de red si desea abrir un amplio acceso a varios puertos y direcciones IP.
- AWS PrivateLink crea puntos de conexión en una subred privada de la VPC y estos puntos de conexión se registran como entradas de DNS en Amazon Route 53 Resolver. Al usar DNS, las aplicaciones pueden resolver los puntos de conexión y conectarse a los servicios registrados, sin la necesidad de puertas de enlace NAT o puertas de enlace de Internet en la VPC.
- Amazon VPC Lattice asocia servicios, como aplicaciones, a varias cuentas y VPC y los recopila en una red de servicios. Los clientes de las VPC asociadas a la red de servicios pueden enviar solicitudes a todos los demás servicios asociados a la red de servicios, independientemente de si se encuentran en la misma cuenta o no. VPC Lattice se integra con AWS Resource Access Manager (AWS RAM) para que pueda compartir recursos con otras cuentas o a través de ellas. AWS Organizations Puede asociar una VPC a una sola red de servicio. Esta solución no requiere el uso de interconexiones de VPC o AWS Transit Gateway para comunicarse entre cuentas.

Prácticas recomendadas para la conectividad de red

- Cree una Cuenta de AWS que utilice para la red centralizada. Asigne el nombre network-prod a esta cuenta y utilícela para AWS Transit Gateway Amazon VPC IP Address Manager (IPAM). Agregue esta cuenta a la unidad organizativa Infrastructure_Prod.
- Utilice AWS Resource Access Manager (AWS RAM) para compartir la puerta de enlace de tránsito, las redes de servicios de VPC Lattice y los grupos de IPAM con el resto de la organización. Esto permite que cualquier miembro Cuenta de AWS de su organización interactúe con estos servicios.
- Al utilizar los grupos de IPAM para administrar de forma centralizada las asignaciones de direcciones IPv4 e IPv6, puede permitir que sus usuarios finales aprovisionen las VPC por sí mismos mediante AWS Service Catalog. Esto lo ayuda a dimensionar las VPC de forma adecuada y a evitar la superposición de espacios de direcciones IP.
- Utilice un enfoque de salida centralizado para el tráfico vinculado a Internet y un enfoque de entrada descentralizado para el tráfico que llegue a su entorno desde Internet. Para obtener más información, consulte Salida centralizada y Entrada descentralizada.

Salida centralizada

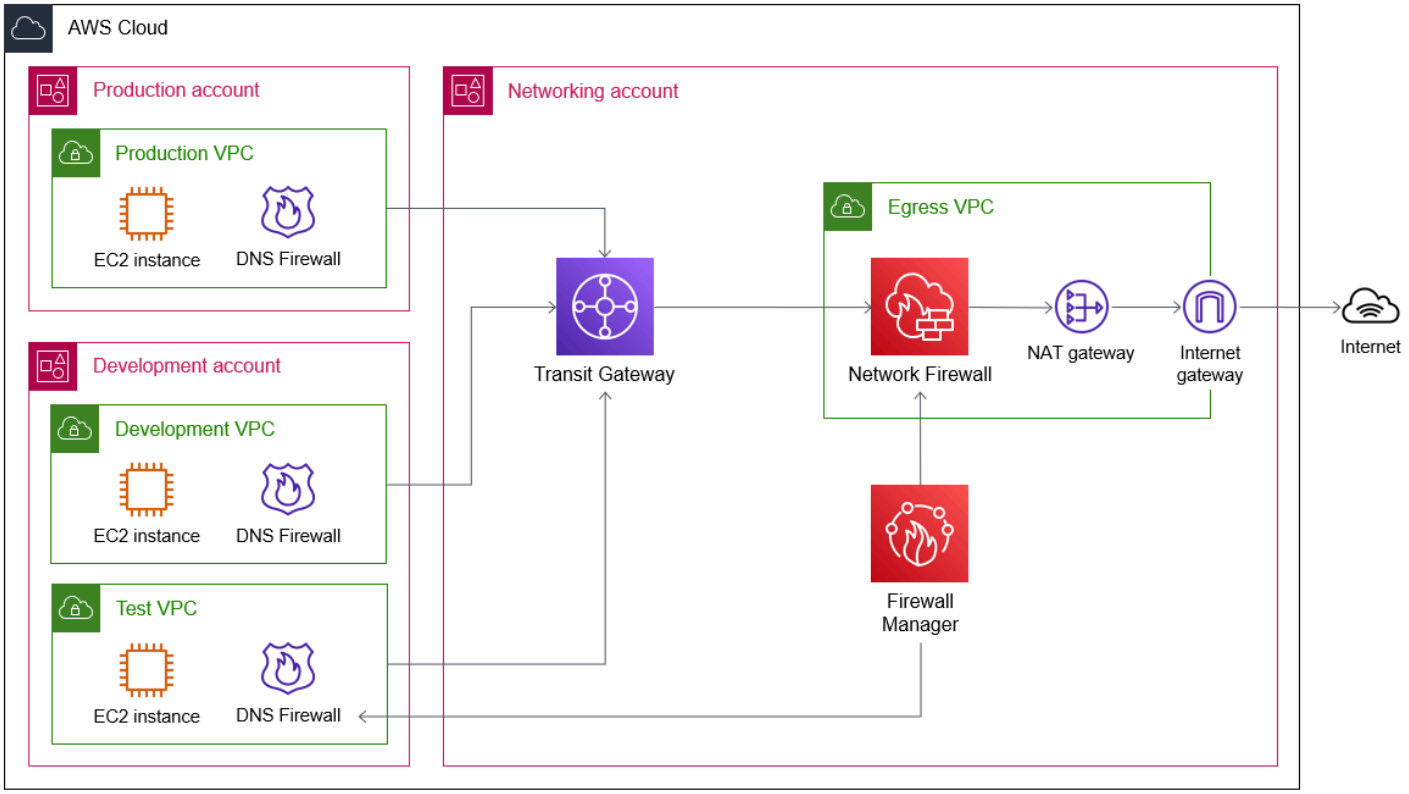
La salida centralizada es el principio de utilizar un punto de inspección único y común para todo el tráfico de red destinado a Internet. En este punto de inspección, puede permitir el tráfico solo a dominios específicos o solo a través de puertos o protocolos específicos. La centralización de la

salida también puede ayudarlo a reducir los costos al eliminar la necesidad de implementar puertas de enlace NAT en cada una de sus VPC para poder alcanzar Internet. Esto es beneficioso desde el punto de vista de la seguridad, ya que limita la exposición a recursos maliciosos de acceso externo, como la infraestructura de comando y control (CyC) de malware. Para obtener más información y opciones de arquitectura para la salida centralizada, consulte la salida centralizada a Internet (documentoAWS técnico).

Puede usar AWS Network Firewall, que es un firewall de red administrado y con estado y un servicio de detección y prevención de intrusiones, como punto de inspección central del tráfico de salida. Este firewall se configura en una VPC dedicada para el tráfico de salida. Network Firewall admite reglas con estado que puede usar para limitar el acceso a Internet a dominios específicos. Para obtener más información, consulte Filtrado de dominios(documentación de Network Firewall).

También puede usar Firewall de DNS de Amazon Route 53 Resolver para limitar el tráfico de salida a nombres de dominio específicos, principalmente para evitar la exfiltración no autorizada de sus datos. En las reglas del firewall de DNS, puede aplicar listas de dominios (documentación de Route 53), que permiten o deniegan el acceso a dominios específicos. Puede utilizar listas de dominios AWS gestionadas, que contienen nombres de dominio asociados a actividades malintencionadas u otras amenazas potenciales, o puede crear listas de dominios personalizadas. Puede crear grupos de reglas de firewall de DNS y, a continuación, aplicarlos a sus VPC. Las solicitudes de DNS salientes se enrutan a través de un Resolver en la VPC para la resolución de nombres de dominio, y el firewall de DNS filtra las solicitudes en función de los grupos de reglas aplicados a la VPC. Las solicitudes de DNS recursivas que se envían al Resolver no fluyen a través de la puerta de enlace de tránsito ni de la ruta de Network Firewall. Route 53 Resolver y el firewall de DNS deben considerarse una ruta de salida independiente de la VPC.

En la imagen siguiente, se muestra un ejemplo de arquitectura para salida centralizada. Antes de que comience la comunicación de red, las solicitudes de DNS se envían al Route 53 Resolver, donde el firewall de DNS permite o deniega la resolución de la dirección IP utilizada para la comunicación. El tráfico destinado a Internet se enruta a una puerta de enlace de tránsito en una cuenta de red centralizada. La puerta de enlace de tránsito reenvía el tráfico a Network Firewall para su inspección. Si la política de firewall permite el tráfico de salida, el tráfico pasa a través de una puerta de enlace NAT, a través de una puerta de enlace de Internet y se luego a Internet. Puede usarlo AWS Firewall Manager para administrar de forma centralizada los grupos de reglas del Firewall de DNS y las políticas de Network Firewall en toda su infraestructura de cuentas múltiples.



Prácticas recomendadas para proteger el tráfico de salida

- Comience en modo de solo registro (documentación de Route 53). Cambie al modo de bloqueo después de haber validado que el tráfico legítimo no se ve afectado.
- Bloquee el tráfico de DNS que va a Internet mediante AWS Firewall Manager políticas para las listas de control de acceso a la red o mediante AWS Network Firewall. Todas las consultas de DNS deben enrutarse a través de un Route 53 Resolver, donde puede supervisarlas con Amazon GuardDuty (si está habilitado) y filtrarlas con el firewall DNS de Route 53 Resolver (si está habilitado). Para obtener más información, consulte Resolución de consultas de DNS entre las VPC y la red (documentación de Route 53).
- Utilice las Listas de dominios administradas de AWS (documentación de Route 53) en firewall de DNS y Network Firewall.
- Considere bloquear los dominios de nivel superior no utilizados y de alto riesgo, como .info, .top, .xyz o algunos dominios de código de país.
- Considere bloquear los puertos no utilizados y de alto riesgo, como los puertos 1389, 4444, 3333, 445, 135, 139 o 53.

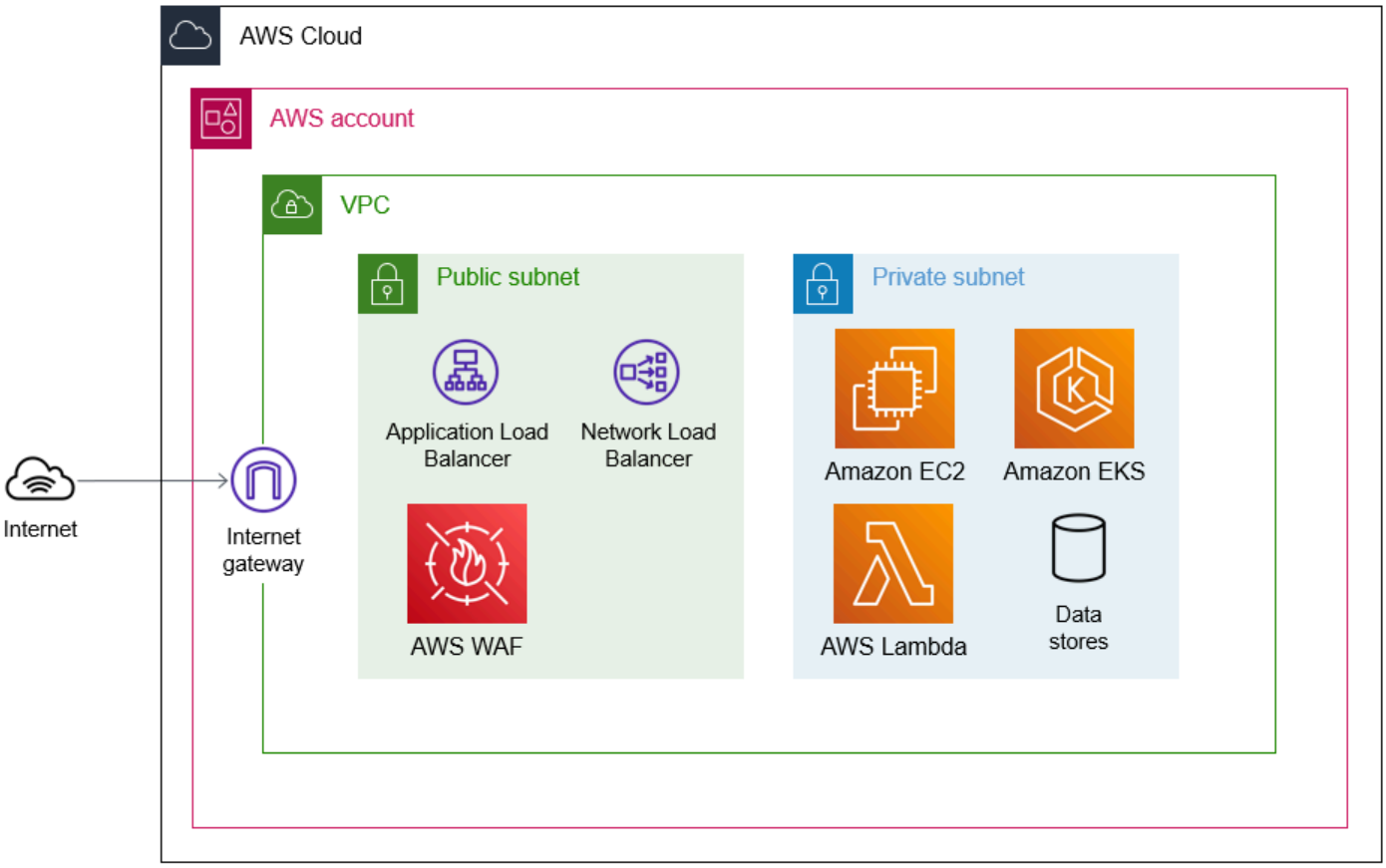
- Como punto de partida, puede utilizar una lista de denegaciones que incluya las reglas AWS gestionadas. A continuación, podrá trabajar poco a poco para implementar un modelo de lista de permitidos. Por ejemplo, en lugar de incluir solo una lista estricta de nombres de dominio totalmente cualificados en la lista de dominios permitidos, comience por utilizar algunos caracteres comodín, como *.example.com. Incluso puedes permitir solo los dominios de nivel superior que esperes y bloquear todos los demás. Luego, con el tiempo, redúzcalos también.
- Utilice los perfiles de Route 53 (documentación de Route 53) para aplicar las configuraciones de Route 53 relacionadas con el DNS en muchas VPC y en diferentes. Cuentas de AWS
- Defina un proceso para gestionar las excepciones a estas mejores prácticas.

Entrada descentralizada

La entrada descentralizada es el principio que define, a nivel de cuenta individual, cómo el tráfico de Internet llega a las cargas de trabajo de esa cuenta. En las arquitecturas de varias cuentas, una de las ventajas de la entrada descentralizada es que cada cuenta puede usar el servicio o recurso de entrada más adecuado para sus cargas de trabajo, como un equilibrador de carga de aplicación, Amazon API Gateway o un Equilibrador de carga de red.

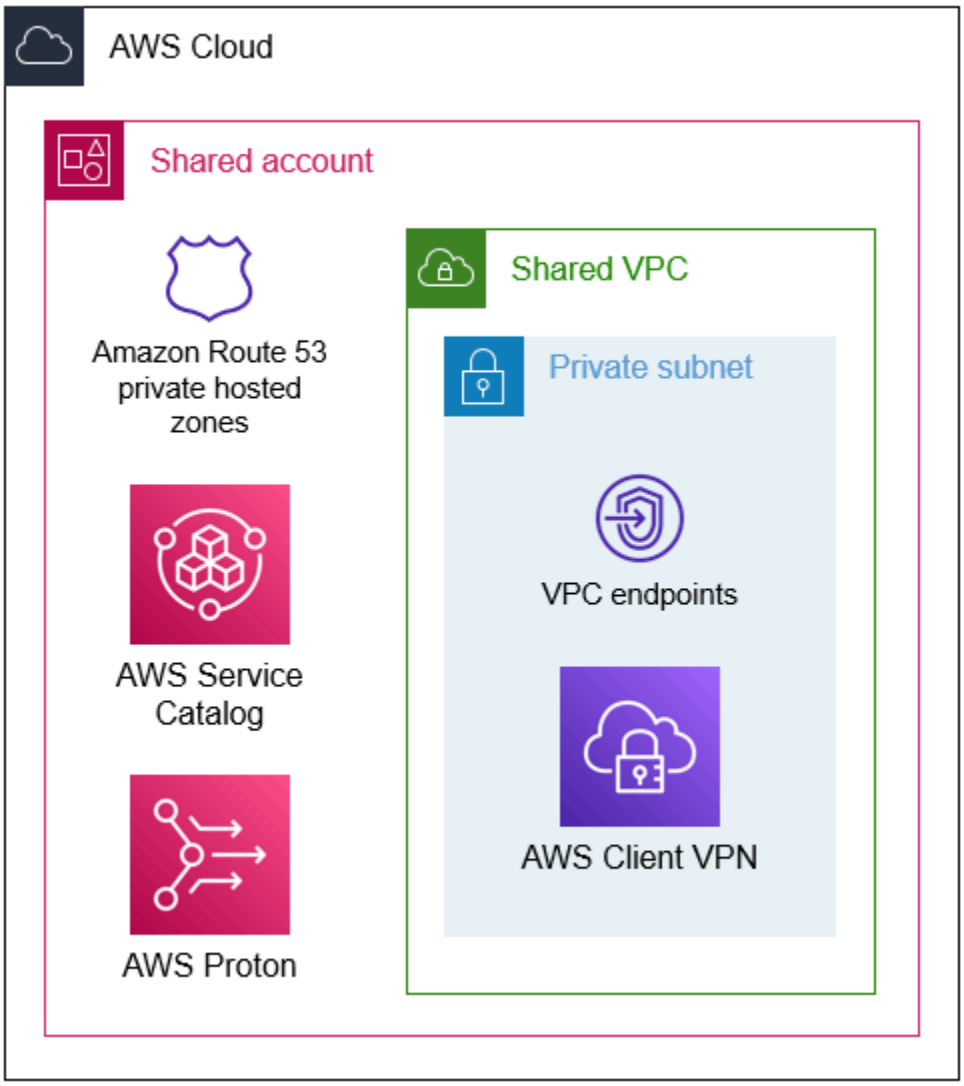
Si bien el ingreso descentralizado significa que debe administrar cada cuenta de forma individual, puede administrar y mantener sus configuraciones de forma centralizada mediante AWS Firewall Manager. Firewall Manager admite protecciones como AWS WAF y Grupos de seguridad de Amazon VPC. Puede asociarse AWS WAF a un Application Load Balancer CloudFront, Amazon, API Gateway o. AWS AppSync Si utiliza una VPC de salida y una puerta de enlace de tránsito, como se describe en Salida centralizada, cada VPC de radio contiene subredes públicas y privadas. Sin embargo, no es necesario implementar puertas de enlace NAT porque el tráfico se enruta a través de la VPC de salida de la cuenta de red.

La siguiente imagen muestra un ejemplo de una persona Cuenta de AWS que tiene una sola VPC que contiene una carga de trabajo accesible a través de Internet. El tráfico de Internet accede a la VPC a través de una puerta de enlace de Internet y llega a los servicios de equilibrio de carga y seguridad alojados en una subred pública. (Una subred pública contiene una ruta predeterminada hacia una puerta de enlace de Internet). Implemente balanceadores de carga en subredes públicas y adjunte listas de control de AWS WAF acceso (ACL) para protegerse del tráfico malintencionado, como las secuencias de comandos entre sitios. Implemente cargas de trabajo que alojen aplicaciones en subredes privadas, que no tienen acceso directo a Internet ni desde ella.



Si tiene muchas VPC en su organización, es posible que desee compartir Servicios de AWS comunes mediante la creación de puntos de conexión de VPC de interfaz o zonas alojadas privadas en una Cuenta de AWS dedicada y compartida. Para obtener más información, consulte Acceder y Servicio de AWS utilizar un punto final de VPC de interfaz (AWS PrivateLink documentación) y Trabajar con zonas alojadas privadas (documentación de Route 53).

La siguiente imagen muestra un ejemplo de una Cuenta de AWS que aloja recursos que se pueden compartir en toda la organización. Los puntos de conexión de VPC se pueden compartir en varias cuentas al crearlos en una VPC dedicada. Al crear un punto de conexión de VPC, de forma opcional, puede hacer que AWS administre las entradas de DNS del punto de conexión. Para compartir un punto de conexión, desactive esta opción y cree las entradas de DNS en una zona alojada privada (PHZ) de Route 53 independiente. De esta manera, puede asociar la PHZ a todas las VPC de su organización para obtener una resolución de DNS centralizada de los puntos de conexión de VPC. También debe asegurarse de que las tablas de enrutamiento de la puerta de enlace de tránsito incluyan rutas de la VPC compartida a las demás VPC. Para obtener más información, consulte Acceso centralizado a los puntos finales de la interfaz de la VPC (AWS documento técnico).



Un sitio compartido también Cuenta de AWS es un buen lugar para alojar carteras. AWS Service Catalog Una cartera es un conjunto de servicios de TI en los que desea que estén disponibles para su implementación AWS, y la cartera contiene información de configuración de esos servicios. Puede crear las carteras en la cuenta compartida, compartirlas con la organización y, a continuación, cada cuenta de miembro importa la cartera a su propia instancia regional de Service Catalog. Para obtener más información, consulte Compartir con AWS Organizations (documentación de Service Catalog).

Del mismo modo AWS Proton, con la cuenta compartida puede administrar de forma centralizada el entorno y las plantillas de servicios y, a continuación, configurar las conexiones de las cuentas con las cuentas de los miembros de la organización. Para obtener más información, consulte Conexiones de cuentas de entorno (AWS Proton documentación).

Respuesta a incidentes de seguridad para una arquitectura de varias cuentas

A medida que realiza la transición a varios Cuentas de AWS, es importante que mantenga la visibilidad de los eventos de seguridad que puedan producirse en su organización. En Administración de identidades y control de acceso, usted usó AWS Control Tower para configurar su zona de aterrizaje. Durante ese proceso de configuración, AWS Control Tower designó un Cuenta de AWS hombre de seguridad. Debe delegar la administración de los servicios de seguridad en la security-tooling-prodcuenta y utilizarla para gestionar estos servicios de forma centralizada.

En esta guía se analiza el uso de lo siguiente Servicios de AWS para ayudar a proteger su organización Cuentas de AWS y su organización:

- Amazon GuardDuty
- Amazon Macie
- AWS Security Hub

Amazon GuardDuty

Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza las fuentes de datos, como los registros de AWS CloudTrail eventos. Para obtener una lista completa de las fuentes de datos compatibles, consulta Cómo GuardDuty utiliza Amazon sus fuentes de datos (GuardDuty documentación). Utiliza fuentes de información de amenazas, como listas de direcciones IP y dominios maliciosos, y machine learning para identificar la actividad inesperada y potencialmente no permitida, así como la actividad maliciosa en su entorno de AWS .

Si la usas GuardDuty con AWS Organizations, la cuenta de administración de la organización puede designar cualquier cuenta de la organización como administradora GuardDuty delegada. El administrador delegado se convierte en la cuenta de GuardDuty administrador de la región. GuardDuty se habilita automáticamente cuando:Región de AWS, y la cuenta de administrador delegado tiene permisos para habilitar y administrar GuardDuty todas las cuentas de la organización dentro de esa región. Para obtener más información, consulte Administrar GuardDuty cuentas con AWS Organizations (GuardDuty documentación).

GuardDuty es un servicio regional. Esto significa que debe habilitarlo GuardDuty en cada región que desee supervisar.

Prácticas recomendadas

- Se admiten todas GuardDuty las opciones habilitadas Regiones de AWS. GuardDuty puede generar información sobre actividades no autorizadas o inusuales, incluso en las regiones que no utilizas activamente. Los precios GuardDuty se basan en la cantidad de eventos analizados. Incluso en las regiones en las que no se utilizan cargas de trabajo, la activación GuardDuty es una herramienta de detección eficaz y rentable que le avisa sobre posibles actividades maliciosas. Para obtener más información sobre las regiones en las que GuardDuty está disponible, consulta los puntos de enlace GuardDuty de servicio de Amazon (Referencia general de AWS).
- En cada región, delega la administración GuardDuty de la security-tooling-prodcuenta en tu organización. Para obtener más información, consulte Designación de un administrador GuardDuty delegado (GuardDuty documentación).
- Configure GuardDuty para inscribir automáticamente a los nuevos a Cuentas de AWS medida que se agreguen a la organización. Para obtener más información, consulte el paso 3: automatizar la adición de nuevas cuentas de la organización como miembros en Administrar cuentas con AWS Organizations (GuardDuty documentación).

Amazon Macie

Amazon Macie es un servicio de seguridad y privacidad de datos completamente administrado que utiliza machine learning y coincidencia de patrones para descubrir, monitorear y ayudar a proteger sus datos confidenciales en Amazon Simple Storage Service (Amazon S3). Puede exportar datos de Amazon Relational Database Service (Amazon RDS) y Amazon DynamoDB a un bucket de S3 y luego utilizar Macie para escanear los datos.

Si utiliza Macie con AWS Organizations, la cuenta de administración de la organización puede designar cualquier cuenta de la organización como cuenta de administrador de Macie. La cuenta de administrador puede habilitar y administrar Macie para las cuentas de los miembros de la organización, puede acceder a los datos de inventario de Amazon S3 y puede ejecutar tareas de descubrimiento de datos confidenciales para las cuentas. Para obtener más información, consulte Administración de cuentas con AWS Organizations (documentación de Macie).

Macie es un servicio regional. Esto significa que debe habilitar Macie en cada región que desee monitorear y que la cuenta de administrador de Macie solo puede administrar las cuentas de los miembros dentro de la misma región.

Prácticas recomendadas

- Siga las Consideraciones y recomendaciones para usar Macie con AWS Organizations (documentación de Macie).
- En cada región, delegue la security-tooling-prodcuenta para administrar Macie en su organización. Para gestionar de forma centralizada las cuentas de Macie en varias Regiones de AWS, la cuenta de administración debe iniciar sesión en cada región en la que la organización utilice o vaya a utilizar Macie y, a continuación, designar la cuenta de administrador de Macie en cada una de esas regiones. De esa forma, la cuenta de administrador de Macie puede configurar la organización en cada una de esas regiones. Para obtener más información, consulte Integración y configuración de una organización (documentación de Macie).
- Macie ofrece un nivel gratuito mensual para trabajos de detección de datos confidenciales. Si tiene datos confidenciales almacenados en Amazon S3, utilice Macie para analizar sus buckets de S3 como parte del nivel mensual gratuito. Si supera el nivel gratuito, se empezarán a acumular cargos por el descubrimiento de datos confidenciales en su cuenta.

AWS Security Hub

AWS Security Hublo proporciona una visión completa del estado de su seguridad en. AWS Su uso le permite comprobar su entorno con los estándares y las prácticas recomendadas del sector de seguridad. Security Hub recopila datos de seguridad de todos sus Cuentas de AWS servicios (incluidos GuardDuty Macie) y de los productos de socios externos compatibles. Security Hub lo ayuda a analizar sus tendencias de seguridad y a identificar los problemas de seguridad de mayor prioridad. Security Hub brinda varios estándares de seguridad que puede habilitar para realizar comprobaciones de conformidad en cada Cuenta de AWS.

Si utiliza Security Hub con AWS Organizations, la cuenta de administración de la organización puede designar cualquier cuenta de la organización como cuenta de administrador del Security Hub. De esta forma, la cuenta de administrador de Security Hub puede habilitar y administrar las cuentas de otros miembros de la organización. Para obtener más información, consulte Uso AWS Organizations para administrar cuentas (documentación de Security Hub).

Security Hub es un servicio regional. Esto significa que debe habilitar Security Hub en cada región que desee analizar y, en ella AWS Organizations, debe definir el administrador delegado para cada región.

Prácticas recomendadas

- Siga los Requisitos previos y recomendaciones (documentación de Security Hub).
- En cada región, delegue la security-tooling-prodcuenta para administrar Security Hub para su organización. Para obtener más información, consulte Designación de una cuenta de administrador de Security Hub (documentación de Security Hub).
- Configure Security Hub para que inscriba automáticamente a los nuevos Cuentas de AWS cuando se agreguen a la organización.
- Habilite el Estándar de prácticas de seguridad recomendadas fundamentales de AWS (documentación de Security Hub) para detectar cuándo los recursos se desvían de estas prácticas.
- Habilite Agregación entre regiones (documentación del Security Hub) para que pueda ver y administrar todos los resultados de Security Hub desde una única región.

Configuración de copias de seguridad para una arquitectura de varias cuentas

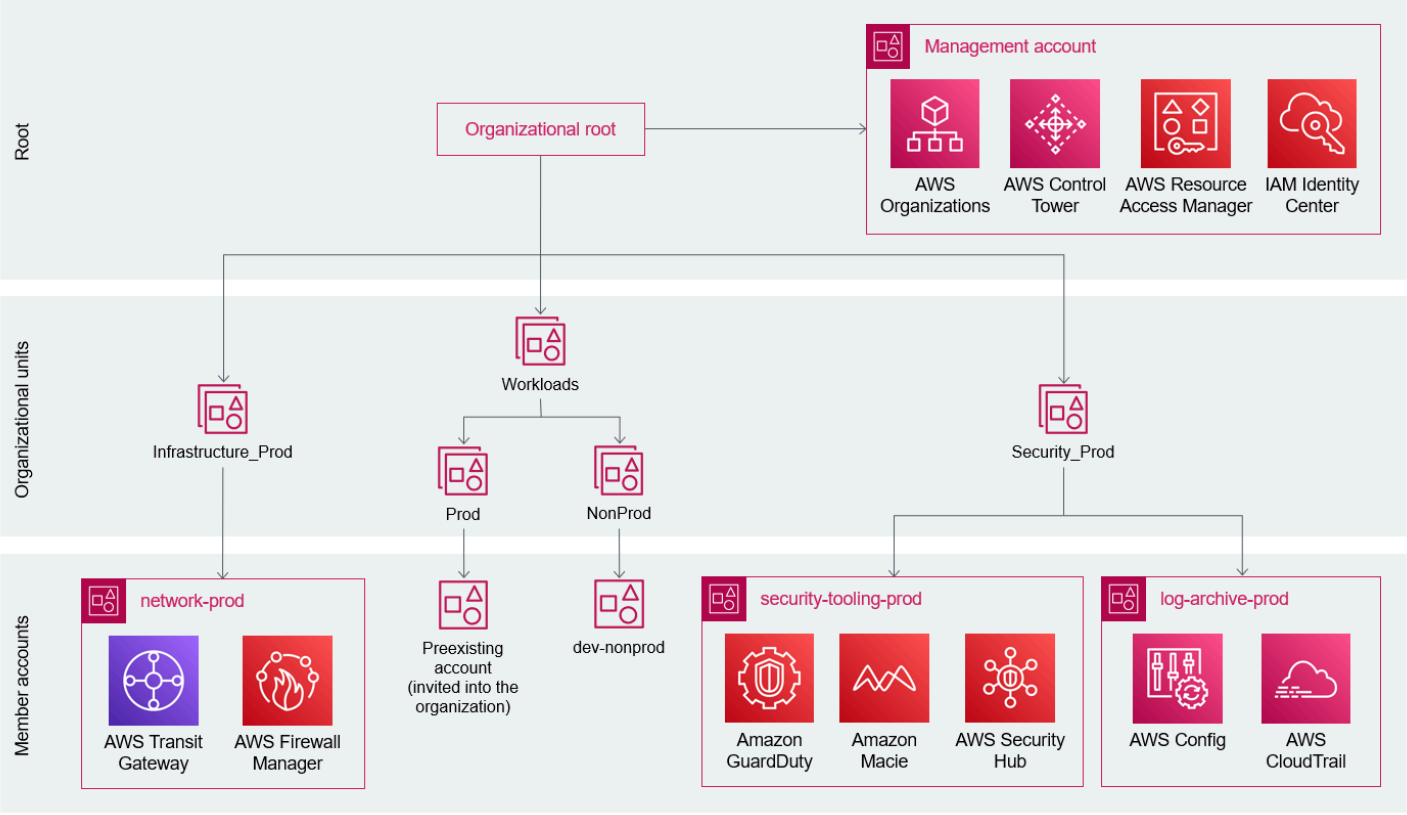
Una estrategia de copias de seguridad integral es una parte esencial del plan de protección de datos de una empresa para resistir, recuperar y reducir cualquier impacto que pueda sufrir debido a un incidente de seguridad. Una política de copia de seguridad lo ayuda a estandarizar e implementar una estrategia de copias de seguridad de los recursos de todas las cuentas de su organización. En una Política de copia de seguridad, puede configurar e implementar planes de copia de seguridad para sus recursos. Para obtener más información, consulte Políticas de copia de seguridad (documentación de AWS Organizations). Para obtener más información, consulte Las 10 prácticas de seguridad recomendadas para proteger las copias de seguridad en AWS (Recomendaciones de AWS).

Migración de cuentas al realizar la transición a una arquitectura de varias cuentas

En Invitación a su cuenta preexistente, ha invitado a su cuenta preexistente a unirse a la unidad organizativa Cargas de trabajo > Prod. Esta cuenta ahora se administra como parte de su organización.

También ha aprovisionado una nueva cuenta dev-nonprod en la unidad organizativa Cargas de trabajo > NonProd. Los miembros del equipo ahora deberían poder acceder a las cuentas correspondientes a través de AWS IAM Identity Center. Elimine cualquier cuenta de usuario individual en AWS Identity and Access Management (IAM).

Si ha seguido las recomendaciones de esta guía, ahora su organización tiene la siguiente estructura.



Si hay cargas de trabajo ejecutándose en la cuenta preexistente, ahora puede migrarlas a cuentas independientes, de acuerdo con los criterios que estableció en Configuración de los criterios de alcance. Migre cualquier carga de trabajo que no sea de producción a la nueva unidad organizativa dev-nonprod y migre las cargas de trabajo de producción a la cuenta network-prod. Para obtener

más información sobre la migración de recursos comunes de AWS, consulte la siguiente sección de esta guía, Migración de recursos.

Replicación o migración de recursos entre Cuentas de AWS

Tras migrar de una arquitectura de una sola cuenta Cuenta de AWS a una arquitectura de varias cuentas, es habitual que las cargas de trabajo de producción y de no producción se ejecuten en la cuenta preexistente. La migración de estos recursos a cuentas de producción y no producción dedicadas o unidades organizativas lo ayuda a administrar el acceso y las redes para estas cargas de trabajo. Las siguientes son algunas opciones para migrar recursos comunes a otros. AWS Cuenta de AWS

Esta sección se centra en las estrategias para replicar datos entre Cuentas de AWS. Debe intentar que sus cargas de trabajo en la mayor medida posible no tenga estado para evitar tener que replicar los recursos de computación entre cuentas. También resulta útil administrar los recursos mediante infraestructura como código (IaC) para poder reaprovisionar un entorno en una Cuenta de AWS independiente.

En esta sección, se analizan las opciones para migrar los siguientes recursos de datos:

- AWS AppConfig configuraciones y entornos
- AWS Certificate Manager certificados
- CloudFront Distribuciones de Amazon
- AWS CodeArtifact dominios y repositorios
- Tablas de Amazon DynamoDB
- EBSVolúmenes de Amazon
- EC2instancias de Amazon o AMIs
- ECRRegistros de Amazon
- Sistemas de EFS archivos de Amazon
- Clústeres de Amazon ElastiCache (RedisOSS)
- AWS Elastic Beanstalk entornos
- Direcciones IP elásticas
- AWS Lambda capas
- Instancias de Amazon Lightsail
- Clústeres de Amazon Neptune
- Dominios OpenSearch de Amazon Service
- RDSInstantáneas de Amazon

- Clústeres de Amazon Redshift
- Dominios y zonas alojadas de Amazon Route 53
- Buckets de Amazon S3
- SageMaker Modelos de Amazon
- AWS WAF web ACLs

AWS AppConfig configuraciones y entornos

AWS AppConfig no admite la copia directa de su configuración a otra Cuenta de AWS. Sin embargo, se recomienda administrar las AWS AppConfig configuraciones y los entornos por separado de los Cuentas de AWS que alojan los entornos. Para obtener más información, consulte Configuración multicuenta con AWS AppConfig (AWS entrada del blog).

AWS Certificate Manager certificados

No puedes exportar directamente un certificado AWS Certificate Manager (ACM) de una cuenta a otra porque la clave AWS Key Management Service (AWS KMS) que se utiliza para cifrar la clave privada del certificado es única para cada Región de AWS cuenta. Sin embargo, puede aprovisionar de forma simultánea varios certificados con el mismo nombre de dominio en varias cuentas y regiones. ACMpermite validar la propiedad del dominio mediante DNS (recomendado) o el correo electrónico. Al utilizar la DNS validación y crear un certificado nuevo, ACM genera un CNAME registro único para cada dominio del certificado. El CNAME registro es único para cada cuenta y debe añadirse a la zona alojada o al DNS proveedor de Amazon Route 53 en un plazo de 72 horas para que el certificado se valide correctamente.

CloudFront Distribuciones de Amazon

Amazon CloudFront no admite la migración de distribuciones de una Cuenta de AWS a otra Cuenta de AWS. Sin embargo, CloudFront admite la migración de un nombre de dominio alternativo, también conocido como a CNAME, de una distribución a otra. Para obtener más información, consulte Cómo se resuelve el CNAMEAlreadyExists error al configurar un CNAME alias para mi CloudFront distribución (AWS Knowledge Center).

AWS CodeArtifact dominios y repositorios

Si bien una organización puede tener varios dominios, se recomienda tener un único dominio de producción que contenga todos los artefactos publicados. Esto ayuda a los equipos de desarrollo a encontrar y compartir paquetes en una organización. La Cuenta de AWS cuenta propietaria del dominio puede ser diferente de la cuenta propietaria de los repositorios asociados al dominio. Puede copiar paquetes entre repositorios siempre y cuando pertenezcan al mismo dominio. Para obtener más información, consulte Copiar paquetes entre repositorios (CodeArtifact documentación).

Tablas de Amazon DynamoDB

Puede utilizar uno de los siguientes servicios para migrar una tabla de Amazon DynamoDB a otra Cuenta de AWS:

- AWS Backup
- Importar y exportar de DynamoDB a Amazon S3
- Amazon S3 y AWS Glue
- AWS Data Pipeline
- Amazon EMR

Para obtener más información, consulte Cómo puedo migrar mis tablas de Amazon DynamoDB de Cuenta de AWS una a otra AWS (Knowledge Center).

EBSVolúmenes de Amazon

Puede tomar una instantánea de un volumen existente de Amazon Elastic Block Store (AmazonEBS), compartir la instantánea con la cuenta de destino y, a continuación, crear una copia del volumen en la cuenta de destino. De este modo, el volumen migra de manera eficaz de una cuenta a otra. Para obtener más información, consulte Cómo puedo compartir un volumen o una EBS instantánea de Amazon cifrados con otra persona Cuenta de AWS (AWS Knowledge Center).

EC2instancias de Amazon o AMIs

No es posible transferir directamente las instancias existentes de Amazon Elastic Compute Cloud (AmazonEC2) o Amazon Machine Images (AMIs) a una instancia diferente Cuenta de AWS. En su

lugar, puede crear una cuenta personalizada AMI en la cuenta de origen, compartirla AMI con la cuenta de destino, lanzar una nueva EC2 instancia desde la cuenta compartida AMI de la cuenta de destino y, a continuación, anular el registro de la compartida. AMI Para obtener más información, consulta Cómo transfiero una EC2 instancia de Amazon o AMI a otra Cuenta de AWS (AWS Knowledge Center).

ECRRegistros de Amazon

Amazon Elastic Container Registry (AmazonECR) admite la replicación entre cuentas y regiones. La replicación se configura en el registro de origen y una política de permisos de registro en el registro de destino. Para obtener más información, consulte Configuración de la replicación multicuenta (ECRdocumentación de Amazon) y Permitir que el usuario raíz de una cuenta de origen replique todos los repositorios (ECRdocumentación de Amazon).

Sistemas de EFS archivos de Amazon

En el caso de Amazon Elastic File System (AmazonEFS), se puede utilizar AWS DataSync para copiar datos de un sistema de archivos de origen a un sistema de archivos de destino de otro Cuenta de AWS. El DataSync agente debe crearse en el mismo sistema de archivos Región de AWS y Cuenta de AWS en el sistema de archivos de origen. Para obtener más información, consulte Transferir datos de un sistema de archivos en la nube a otro sistema de archivos en la nube (DataSyncdocumentación). Al copiar entre dos sistemas de EFS archivos de Amazon distintos Cuentas de AWS, te recomendamos que utilices la transferencia NFS (de origen) a EFS (destino). Para obtener más información e instrucciones, consulta Crear una tarea para transferir datos desde Amazon EFS (DataSync documentación).

Clústeres de Amazon ElastiCache (RedisOSS)

Puede utilizar una copia de seguridad de un clúster de base de datos de Amazon ElastiCache (RedisOSS) para migrarlo a una cuenta diferente. Para obtener más información, consulte Cuáles son las mejores prácticas para migrar mi clúster ElastiCache (RedisOSS) (AWS Knowledge Center).

AWS Elastic Beanstalk entornos

Para ello AWS Elastic Beanstalk, puede utilizar las configuraciones guardadas (documentación de Elastic Beanstalk) para migrar un entorno a otro. Cuenta de AWS Para obtener más información,

consulte Cómo migro mi entorno de Elastic Beanstalk Cuenta de AWS de uno Cuenta de AWS a AWS otro (Knowledge Center).

Direcciones IP elásticas

Puede transferir direcciones IP elásticas entre direcciones IP Cuentas de AWS que estén en el mismo lugar. Región de AWS Para obtener más información, consulte Transferir direcciones IP elásticas (VPCdocumentación de Amazon).

AWS Lambda capas

De forma predeterminada, AWS Lambda la capa que cree es privada para su Cuenta de AWS. Sin embargo, si lo desea, puede compartir la capa con otras personas Cuentas de AWS o hacerla pública. Para copiar una capa, debe volver a aprovisionarla en otra Cuenta de AWS. Para obtener más información, consulte Configuración de permisos de capa (documentación de Lambda).

Instancias de Amazon Lightsail

Puede crear una instantánea de una instancia de Amazon Lightsail y exportarla a una Amazon Machine Image AMI () y a una instantánea cifrada de un volumen de Amazon. EBS Para obtener más información, consulte Exportación de instantáneas de Amazon Lightsail a Amazon EC2 (documentación de Lightsail). De forma predeterminada, la instantánea se cifra con una clave AWS gestionada creada en (). AWS Key Management Service AWS KMS Sin embargo, este tipo de KMS clave no se puede compartir entre ellos Cuentas de AWS. En su lugar, se cifra manualmente una copia de la misma AMI con una clave gestionada por el cliente que se puede utilizar desde la cuenta de destino. Para obtener más información, consulte Permitir que los usuarios de otras cuentas usen una KMS clave (AWS KMS documentación). A continuación, puede compartir la copia AMI con el objetivo Cuenta de AWS y lanzar una nueva EC2 instancia para Lightsail a partir de la copia. AMI Para obtener más información, consulte Lanzar una instancia mediante el asistente de lanzamiento de nuevas instancias (EC2documentación de Amazon).

Clústeres de Amazon Neptune

Puede copiar una instantánea automática del clúster de base de datos de Amazon Neptune en otra Cuenta de AWS. Para obtener más información, consulte Copiar una instantánea de un clúster de base de datos (DB) (documentación de Neptune).

También puede compartir una instantánea manual con un máximo de 20 Cuentas de AWS que puede restaurar un clúster de base de datos directamente a partir de la instantánea. Para obtener más información, consulte Compartir una instantánea de clúster de base de datos (documentación de Neptune).

Dominios OpenSearch de Amazon Service

Para copiar datos entre dominios de Amazon OpenSearch Service, puede utilizar Amazon S3 para crear una instantánea del dominio de origen y, a continuación, restaurar la instantánea en un dominio de destino de otro dominio Cuenta de AWS. Para obtener más información, consulta Cómo restauro datos de un dominio de Amazon OpenSearch Service en otro Cuenta de AWS (AWS Knowledge Center).

Si dispone de conectividad de red entre ellos Cuentas de AWS, también puede utilizar la función de replicación entre clústeres (documentación del OpenSearch servicio) de OpenSearch Service.

RDSInstantáneas de Amazon

En el caso de Amazon Relational Database Service (RDSAmazon), puede compartir instantáneas manuales de instancias o clústeres de bases de datos con un máximo de 20.Cuentas de AWS Puede restaurar un clúster o instancia de base de datos desde una instantánea compartida. Para obtener más información, consulte Cómo comparto instantáneas manuales de Amazon RDS DB o instantáneas de clústeres de base de datos Aurora con otra persona Cuenta de AWS (AWS Knowledge Center).

También puede usar AWS Database Migration Service (AWS DMS) para configurar la replicación continua entre instancias de bases de datos de cuentas diferentes. Sin embargo, esto requiere conectividad de red entre las cuentas, como la VPC interconexión o una pasarela de tránsito.

Clústeres de Amazon Redshift

Para migrar un clúster de Amazon Redshift a otro Cuenta de AWS, debe crear una instantánea manual del clúster en la cuenta de origen, compartir la instantánea con el destino y Cuenta de AWS, a continuación, restaurar el clúster a partir de la instantánea. Para obtener más información, consulte Cómo se copia un clúster aprovisionado de Amazon Redshift a otro Cuenta de AWS (AWS Knowledge Center).

Dominios y zonas alojadas de Amazon Route 53

Puede transferir dominios de Amazon Route 53 entre Cuentas de AWS. Para obtener más información, consulte Transferir un dominio a otra Cuenta de AWS (documentación de Route 53).

También puede migrar una zona alojada de Route 53 a otra. Cuenta de AWS Para obtener más información sobre cuándo esto es recomendable o necesario, consulte Migrar una zona alojada a una Cuenta de AWS diferente (documentación de Route 53). Al migrar una zona alojada, debe volver a crearla en la Cuenta de AWS destino. Para obtener instrucciones, consulte Migración de una zona alojada a una Cuenta de AWS diferente (documentación de Route 53).

Buckets de Amazon S3

Puede utilizar la replicación en la misma región de Amazon Simple Storage Service (Amazon S3) para copiar objetos entre buckets de S3 de la misma región. AWS Para obtener más información, consulte Replicación de objetos (documentación de Amazon S3). Tenga en cuenta lo siguiente:

- Cambie la propiedad de la réplica a la Cuenta de AWS propietaria del bucket de destino. Para obtener instrucciones, consulte Cambiar el propietario de la réplica (documentación de Amazon S3).
- Actualice las condiciones del propietario del bucket para que reflejen el Cuenta de AWS ID del bucket de destino. Para obtener más información, consulte Verificación de la propiedad del bucket con la condición de propietario del bucket (documentación de Amazon S3).
- A partir de abril de 2023, la configuración impuesta por el propietario del bucket estará habilitada para los buckets recién creados, lo que hará que las listas de control de acceso a los buckets (ACLs) y los objetos ACLs resulten ineficaces. Para obtener más información, consulte Los cambios de seguridad de Amazon S3 se avecinan (entrada del AWS blog).
- Puede usar la Replicación por lotes de S3 (documentación de Amazon S3) para replicar objetos que existían antes de configurar la replicación.

SageMaker Modelos de Amazon

SageMaker los modelos se almacenan en un bucket de Amazon S3 durante el entrenamiento. Al conceder acceso al bucket de S3 desde la cuenta destino, puede implementar un modelo almacenado en la cuenta origen en la cuenta destino. Para obtener más información, consulta Cómo

puedo implementar un SageMaker modelo de Amazon en otro Cuenta de AWS (AWS Knowledge Center).

AWS WAF web ACLs

AWS WAF las listas de control de acceso web (webACLs) deben residir en la misma cuenta que los recursos a los que están asociadas, como CloudFront las distribuciones de Amazon, los balanceadores de carga de aplicaciones, Amazon API Gateway y REST APIs AWS AppSync GraphQL. APIs Puede utilizarlas AWS Firewall Manager para administrar la AWS WAF web de forma centralizada ACLs en toda su organización, tanto en AWS Organizations las regiones como entre ellas. Para obtener más información, consulte Introducción a las políticas AWS WAF de AWS Firewall Manager (documentación de Firewall Manager).

Consideraciones de facturación al realizar la transición a una arquitectura de cuentas múltiples

Si la utiliza AWS Organizations para la transición a la facturación múltipleCuentas de AWS, puede utilizar la función de facturación unificada (AWS Organizationsdocumentación). Esta función proporciona una factura única y combinada que muestra los cargos de varias cuentas.

Las siguientes son las mejores prácticas y recomendaciones de facturación para la transición a varias cuentas:

- Si necesitas acceder a tus datos históricos de facturación, antes de aceptar la invitación para unirte a una organización, crea un informe de costes y uso (AWS Cost and Usage Reportdocumentación) para exportar los datos históricos de facturación de la cuenta a un bucket de Amazon Simple Storage Service (Amazon S3). Tras aceptar la invitación para unirse a la organización, ya no se podrá acceder a los datos históricos de facturación de la cuenta.
- Si necesita combinar dos organizaciones, por ejemplo, para una fusión o adquisición, puede utilizar la evaluación de cuentas AWS Organizations (biblioteca de AWS soluciones) para evaluar las políticas basadas en los recursos de cada organización e identificar cualquier posible problema antes de combinarlas.

Conclusión

La transición de una única Cuenta de AWS a varias cuentas puede resultar abrumador al principio si no se cuenta con una estrategia de adopción. Al implementar una estrategia de varias cuentas, puede abordar muchos desafíos a los que se enfrentan las empresas cuando utilizan una única Cuenta de AWS:

- Confundir los datos de producción con los datos de desarrollo: puede habilitar diferentes permisos y accesos mediante AWS IAM Identity Center con conjuntos de permisos separados de unidades organizativas de producción y no producción. Solo los usuarios con altos privilegios deben tener acceso a la base de datos de producción, y ese acceso debe ser auditado y por periodos limitados.
- La implementación de producción afecta otras operaciones comerciales: puede separar a las partes interesadas mediante el uso de varias cuentas y entornos. Por ejemplo, puede crear un entorno de demostración de ventas dedicado dentro de una cuenta que no sea de producción, de modo que pueda planificar las implementaciones y los lanzamientos cuando no se realicen demostraciones.
- Reduzca el rendimiento de las cargas de trabajo de producción al probar las cargas de trabajo de desarrollo: cada Cuenta de AWS tiene cuotas de servicio independientes que gobiernan cada servicio. Al utilizar varias cuentas, puede limitar el alcance de un entorno que afecte a otro entorno.
- Distinguir los costos de producción de los costos de desarrollo: la facturación unificada de la organización acumula todos los costos en el nivel de Cuenta de AWS para que el equipo de finanzas pueda ver cuánto cuesta la producción en comparación con los entornos que no son de producción, como los entornos de desarrollo, pruebas y demostración. También puede usar etiquetas y políticas de etiquetado para separar los costos dentro de una cuenta.
- Limitar el acceso a datos confidenciales: IAM Identity Center le permite disponer de políticas de acceso independientes para un grupo de personas asociadas a una cuenta específica.
- Controlar los costos: al utilizar políticas de control de servicios (SCP) en una arquitectura de varias cuentas, puede impedir el acceso a determinados Servicios de AWS que podrían suponer costos elevados para su organización. Los SCP pueden denegar todo acceso a servicios específicos o pueden limitar el uso de un servicio a un tipo específico, por ejemplo, restringiendo los tipos de instancias de Amazon Elastic Compute Cloud (Amazon EC2) que se pueden crear.

Colaboradores

Los colaboradores de este documento son:

- Justin Plock, arquitecto principal de soluciones, AWS (autor principal)
- Emily Arnautovic, arquitecta principal, AWS
- Jason DiDomenico, arquitecto sénior de soluciones, AWS
- Michael Leighty, arquitecto sénior de soluciones especializado en seguridad, AWS
- Jesse Lepich, arquitecto sénior de soluciones especializado en seguridad, AWS
- Rodney Lester, arquitecto principal de soluciones, AWS
- Israel Lopez Moriano, arquitecto de soluciones, AWS
- George Rolston, arquitecto sénior de soluciones, AWS
- Alex Torres, arquitecto sénior de soluciones, AWS
- Dave Walker, arquitecto principal de soluciones, AWS

Recursos

Recomendaciones de AWS

- Base de seguridad para startups de AWS (SSB de AWS)
- Arquitectura de referencia de seguridad de AWS (SRA de AWS)
- Las 10 prácticas de seguridad recomendadas para proteger las copias de seguridad en AWS

Publicaciones de blog de AWS

- Cómo la configuración de los usuarios y roles de IAM puede ayudar a mantener la seguridad de su startup
- Cómo permitir que los desarrolladores creen recursos de IAM y, al mismo tiempo, mejoren la seguridad y la agilidad de su organización

Documentos técnicos de AWS

- Organización de su entorno de AWS con varias cuentas
- Establezca su base de nube en AWS
- Creación de una infraestructura de red de AWS multiVPC escalable y segura

Ejemplos de código de AWS

- Automatice la configuración de los servicios de seguridad con AWS Control Tower (GitHub)

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
Mejores prácticas de salida centralizada	Hemos actualizado las mejores prácticas para proteger el tráfico de salida.	6 de mayo de 2024
Prácticas recomendadas de organizaciones	Actualizamos las prácticas recomendadas para crear una organización en AWS Organizations.	4 de diciembre de 2023
Consideraciones de facturación	Agregamos la sección Billing considerations.	20 de septiembre de 2023
Migración de recursos, conectividad de aplicaciones y Amazon VPC Lattice	Sumamos las secciones Migración de recursos y Conexión de aplicaciones. También agregamos información sobre un nuevo Servicio de AWS, Amazon Virtual Private Cloud (Amazon VPC) Lattice.	27 de abril de 2023
Historial de la cuenta y ABAC	Hemos revisado la sección Crear una zona de aterrizaje para añadir información sobre cómo garantizar que tu nueva cuenta Cuentas de AWS con un historial de uso para que puedas añadirla a tu zona de AWS Control Tower aterrizaje. También revisamos la sección Agregar usuarios iniciales para	6 de enero de 2023

	agregar información sobre cómo utilizar el control de acceso basado en atributos (ABAC) con el fin de pasar el método de autenticación de un IdP basado en SAML externo a AWS IAM Identity Center.	
Redes de tráfico de salida	Hemos revisado la sección de salida centralizada para añadir información sobre el uso del firewall de Amazon Route 53 Resolver DNS y limitar el tráfico de salida a nombres de dominio específicos.	13 de octubre de 2022
Seguridad del tráfico de salida	Agregamos la sección Prácticas recomendadas para proteger el tráfico de salida.	6 de octubre de 2022
Límites de permisos	Mejoramos la definición de límite de permisos y en la sección Recursos agregamos un nuevo enlace para obtener más información sobre este tema.	22 de septiembre de 2022
Publicación inicial	—	6 de septiembre de 2022

AWS Glosario de orientación prescriptiva

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

Números

Las 7 R

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

- Refactorizar/rediseñar: traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: migre su base de datos Oracle local a la edición compatible con Postgre SQL de Amazon Aurora.
- Redefinir la plataforma (transportar y redefinir): traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Amazon Relational Database Service (RDSAmazon) para Oracle en el. Nube de AWS
- Recomprar (readquirir): cambie a un producto diferente, lo cual se suele llevar a cabo al pasar de una licencia tradicional a un modelo SaaS. Ejemplo: migre su sistema de gestión de relaciones con los clientes (CRM) a Salesforce.com.
- Volver a alojar (migrar mediante lift-and-shift): traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: migre su base de datos Oracle local a Oracle en una EC2 instancia del. Nube de AWS
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma local a un servicio en la nube para la misma plataforma. Ejemplo: migrar una Microsoft Hyper-V aplicación a AWS.
- Retener (revisitar): conserve las aplicaciones en el entorno de origen. Estas pueden incluir las aplicaciones que requieren una refactorización importante, que desee posponer para más adelante, y las aplicaciones heredadas que desee retener, ya que no hay ninguna justificación empresarial para migrarlas.

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

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

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

migración activa-pasiva

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

función agregada

SQLFunción que opera en un grupo de filas y calcula un único valor de retorno para el grupo. Entre los ejemplos de funciones agregadas se incluyen `SUM` y`MAX`.

IA

Véase inteligencia artificial.

AIOps

Consulte las operaciones de inteligencia artificial.

anonimización

El proceso de eliminar permanentemente la información personal de un conjunto de datos. La anonimización puede ayudar a proteger la privacidad personal. Los datos anonimizados ya no se consideran datos personales.

antipatrones

Una solución que se utiliza con frecuencia para un problema recurrente en el que la solución es contraproducente, ineficaz o menos eficaz que una alternativa.

control de aplicaciones

Un enfoque de seguridad que permite el uso únicamente de aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

cartera de aplicaciones

Recopilación de información detallada sobre cada aplicación que utiliza una organización, incluido el costo de creación y mantenimiento de la aplicación y su valor empresarial. Esta información es clave para el proceso de detección y análisis de la cartera y ayuda a identificar y priorizar las aplicaciones que se van a migrar, modernizar y optimizar.

inteligencia artificial (IA)

El campo de la informática que se dedica al uso de tecnologías informáticas para realizar funciones cognitivas que suelen estar asociadas a los seres humanos, como el aprendizaje, la resolución de problemas y el reconocimiento de patrones. Para más información, consulte ¿Qué es la inteligencia artificial?

operaciones de inteligencia artificial (AIOps)

El proceso de utilizar técnicas de machine learning para resolver problemas operativos, reducir los incidentes operativos y la intervención humana, y mejorar la calidad del servicio. Para obtener más información sobre cómo AIOps se utiliza en la estrategia de AWS migración, consulte la guía de integración de operaciones.

cifrado asimétrico

Algoritmo de cifrado que utiliza un par de claves, una clave pública para el cifrado y una clave privada para el descifrado. Puede compartir la clave pública porque no se utiliza para el descifrado, pero el acceso a la clave privada debe estar sumamente restringido.

atomicidad, consistencia, aislamiento, durabilidad () ACID

Conjunto de propiedades de software que garantizan la validez de los datos y la fiabilidad operativa de una base de datos, incluso en caso de errores, cortes de energía u otros problemas.

control de acceso basado en atributos () ABAC

La práctica de crear permisos detallados basados en los atributos del usuario, como el departamento, el puesto de trabajo y el nombre del equipo. Para obtener más información, consulte ABACla AWS documentación de AWS Identity and Access Management (IAM).

origen de datos fidedigno

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

Zona de disponibilidad

Una ubicación distinta dentro de una Región de AWS que está aislada de los fallos en otras zonas de disponibilidad y que proporciona una conectividad de red económica y de baja latencia con otras zonas de disponibilidad de la misma región.

AWS Marco de adopción de la nube ()AWS CAF

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAForganiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y las comunicaciones de las personas a fin de ayudar a la organización a prepararse para una adopción exitosa de la nube. Para obtener más información, consulte el AWS CAFsitio web y el AWS CAFdocumento técnico.

AWS Marco de calificación de la carga de trabajo ()AWS WQF

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQFse incluye con AWS

Schema Conversion Tool ()AWS SCT. Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

B

un bot malo

Un bot destinado a interrumpir o causar daño a personas u organizaciones.

BCP

Consulte la planificación de la continuidad del negocio.

gráfico de comportamiento

Una vista unificada e interactiva del comportamiento de los recursos y de las interacciones a lo largo del tiempo. Puede utilizar un gráfico de comportamiento con Amazon Detective para examinar los intentos de inicio de sesión fallidos, las API llamadas sospechosas y acciones similares. Para obtener más información, consulte Datos en un gráfico de comportamiento en la documentación de Detective.

sistema big-endian

Un sistema que almacena primero el byte más significativo. Véase también endianismo.

clasificación binaria

Un proceso que predice un resultado binario (una de las dos clases posibles). Por ejemplo, es posible que su modelo de ML necesite predecir problemas como “¿Este correo electrónico es spam o no es spam?” o “¿Este producto es un libro o un automóvil?”.

filtro de floración

Estructura de datos probabilística y eficiente en términos de memoria que se utiliza para comprobar si un elemento es miembro de un conjunto.

implementación azul/verde

Una estrategia de despliegue en la que se crean dos entornos separados pero idénticos. La versión actual de la aplicación se ejecuta en un entorno (azul) y la nueva versión de la aplicación en el otro entorno (verde). Esta estrategia le ayuda a revertirla rápidamente con un impacto mínimo.

bot

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

botnet

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

rama

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

acceso con cristales rotos

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

estrategia de implementación sobre infraestructura existente

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

caché de búfer

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

capacidad empresarial

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

planificación de la continuidad del negocio () BCP

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

C

CAF

Consulte el marco AWS de adopción de la nube.

despliegue canario

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

CCoE

Consulte Cloud Center of Excellence.

CDC

Consulte la captura de datos de cambios.

cambiar la captura de datos (CDC)

Proceso de seguimiento de los cambios en un origen de datos, como una tabla de base de datos, y registro de los metadatos relacionados con el cambio. Se puede utilizar CDC para varios fines, como auditar o replicar los cambios en un sistema de destino para mantener la sincronización.

ingeniería del caos

Introducir intencionalmente fallos o eventos disruptivos para poner a prueba la resiliencia de un sistema. Puedes usar AWS Fault Injection Service (AWS FIS) para realizar experimentos que estresen tus AWS cargas de trabajo y evalúen su respuesta.

CI/CD

Consulte la integración continua y la entrega continua.

clasificación

Un proceso de categorización que permite generar predicciones. Los modelos de ML para problemas de clasificación predicen un valor discreto. Los valores discretos siempre son distintos entre sí. Por ejemplo, es posible que un modelo necesite evaluar si hay o no un automóvil en una imagen.

cifrado del cliente

Cifrado de datos localmente, antes de que el objetivo los Servicio de AWS reciba.

Centro de excelencia en la nube (CCoE)

Equipo multidisciplinario que impulsa los esfuerzos de adopción de la nube en toda la organización, incluido el desarrollo de las prácticas recomendadas en la nube, la movilización de recursos, el establecimiento de plazos de migración y la dirección de la organización durante las transformaciones a gran escala. Para obtener más información, consulte las CCoEpublicaciones del blog de estrategia Nube de AWS empresarial.

computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar conectada a la tecnología de computación perimetral.

modelo operativo en la nube

En una organización de TI, el modelo operativo que se utiliza para crear, madurar y optimizar uno o más entornos de nube. Para obtener más información, consulte Creación de su modelo operativo de nube.

etapas de adopción de la nube

Las cuatro fases por las que suelen pasar las organizaciones cuando migran a Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir un CCoE modelo de operaciones)
- Migración: migración de aplicaciones individuales

- Reinvención: optimización de productos y servicios e innovación en la nube

Stephen Orban definió estas etapas en la entrada del blog The Journey Toward Cloud-First & the Stages of Adoption en el blog Nube de AWS Enterprise Strategy. Para obtener información sobre su relación con la estrategia de AWS migración, consulte la guía de preparación para la migración.

CMDB

Consulte la base de datos de administración de la configuración.

repositorio de código

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

caché en frío

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

datos fríos

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

visión artificial (CV)

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

desviación de configuración

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

base de datos de administración de configuración () CMDB

Repositorio que almacena y administra información sobre una base de datos y su entorno de TI, incluidos los componentes de hardware y software y sus configuraciones. Por lo general, se utilizan datos CMDB de una etapa de migración de descubrimiento y análisis de la cartera.

paquete de conformidad

Conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus comprobaciones de conformidad y seguridad. Puede implementar un paquete de conformidad como una entidad única en una Cuenta de AWS región o en una organización mediante una YAML plantilla. Para obtener más información, consulte los paquetes de conformidad en la AWS Config documentación.

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, presentación y producción del proceso de lanzamiento del software. La CI/CD se describe comúnmente como una canalización. La CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Consulte visión artificial.

D

datos en reposo

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

clasificación de datos

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

desviación de datos

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

datos en tránsito

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

malla de datos

Un marco arquitectónico que proporciona una propiedad de datos distribuida y descentralizada con una administración y un gobierno centralizados.

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de bases de datos (DDL)

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

lenguaje de manipulación de bases de datos (DML)

Instrucciones o comandos para modificar (insertar, actualizar y eliminar) la información de una base de datos.

DDL

Consulte el lenguaje de definición de bases de datos.

conjunto profundo

Combinar varios modelos de aprendizaje profundo para la predicción. Puede utilizar conjuntos profundos para obtener una predicción más precisa o para estimar la incertidumbre de las predicciones.

aprendizaje profundo

Un subcampo del ML que utiliza múltiples capas de redes neuronales artificiales para identificar el mapeo entre los datos de entrada y las variables objetivo de interés.

defense-in-depth

Un enfoque de seguridad de la información en el que se distribuyen cuidadosamente una serie de mecanismos y controles de seguridad en una red informática para proteger la confidencialidad, la integridad y la disponibilidad de la red y de los datos que contiene. Al adoptar esta estrategia AWS, se añaden varios controles en diferentes capas de la AWS Organizations estructura para ayudar a proteger los recursos. Por ejemplo, un defense-in-depth enfoque podría combinar la autenticación multifactorial, la segmentación de la red y el cifrado.

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro para administrar las cuentas de la organización y gestionar los permisos de ese servicio. Esta

cuenta se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte Servicios que funcionan con AWS Organizations en la documentación de AWS Organizations .

Implementación

El proceso de hacer que una aplicación, características nuevas o correcciones de código se encuentren disponibles en el entorno de destino. La implementación abarca implementar cambios en una base de código y, a continuación, crear y ejecutar esa base en los entornos de la aplicación.

entorno de desarrollo

Consulte entorno.

control de detección

Un control de seguridad que se ha diseñado para detectar, registrar y alertar después de que se produzca un evento. Estos controles son una segunda línea de defensa, ya que lo advierten sobre los eventos de seguridad que han eludido los controles preventivos establecidos. Para obtener más información, consulte Controles de detección en Implementación de controles de seguridad en AWS.

mapeo del flujo de valor de desarrollo (DVSM)

Proceso que se utiliza para identificar y priorizar las restricciones que afectan negativamente a la velocidad y la calidad en el ciclo de vida del desarrollo de software. DVSMamplía el proceso de mapeo del flujo de valor diseñado originalmente para las prácticas de fabricación ajustada. Se centra en los pasos y los equipos necesarios para crear y transferir valor a través del proceso de desarrollo de software.

gemelo digital

Representación virtual de un sistema del mundo real, como un edificio, una fábrica, un equipo industrial o una línea de producción. Los gemelos digitales son compatibles con el mantenimiento predictivo, la supervisión remota y la optimización de la producción.

tabla de dimensiones

En un esquema en estrella, tabla más pequeña que contiene los atributos de datos sobre los datos cuantitativos de una tabla de hechos. Los atributos de la tabla de dimensiones suelen ser campos de texto o números discretos que se comportan como texto. Estos atributos se utilizan habitualmente para restringir consultas, filtrar y etiquetar conjuntos de resultados.

desastre

Un evento que impide que una carga de trabajo o un sistema cumplan sus objetivos empresariales en su ubicación principal de implementación. Estos eventos pueden ser desastres naturales, fallos técnicos o el resultado de acciones humanas, como una configuración incorrecta involuntaria o un ataque de malware.

recuperación de desastres (DR)

La estrategia y el proceso que se utilizan para minimizar el tiempo de inactividad y la pérdida de datos ocasionados por un desastre. Para obtener más información, consulte Recuperación ante desastres de cargas de trabajo en AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

DML

Consulte el lenguaje de manipulación de bases de datos.

diseño basado en el dominio

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

DR

Consulte recuperación ante desastres.

detección de desviaciones

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

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

computación en la periferia

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

cifrado

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

clave de cifrado

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

endianidad

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

punto de conexión

Consulte el punto final del servicio.

servicio de punto de conexión

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

planificación de recursos empresariales (ERP)

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

cifrado de sobre

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

environment

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

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

epopeya

En las metodologías ágiles, son categorías funcionales que ayudan a organizar y priorizar el trabajo. Las epopeyas brindan una descripción detallada de los requisitos y las tareas de implementación. Por ejemplo, los aspectos más importantes de la AWS CAF seguridad incluyen la gestión de identidades y accesos, los controles de detección, la seguridad de la infraestructura, la protección de datos y la respuesta a incidentes. Para obtener más información sobre las epopeyas en la estrategia de migración de AWS , consulte la Guía de implementación del programa.

ERP

Consulte la planificación de recursos empresariales.

análisis exploratorio de datos () EDA

El proceso de analizar un conjunto de datos para comprender sus características principales. Se recopilan o agregan datos y, a continuación, se realizan las investigaciones iniciales para

encontrar patrones, detectar anomalías y comprobar las suposiciones. EDAse realiza mediante el cálculo de estadísticas resumidas y la creación de visualizaciones de datos.

F

tabla de datos

La tabla central de un esquema en forma de estrella. Almacena datos cuantitativos sobre las operaciones comerciales. Normalmente, una tabla de hechos contiene dos tipos de columnas: las que contienen medidas y las que contienen una clave externa para una tabla de dimensiones.

fallan rápidamente

Una filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de un enfoque ágil.

límite de aislamiento de fallas

En el Nube de AWS, un límite, como una zona de disponibilidad Región de AWS, un plano de control o un plano de datos, que limita el efecto de una falla y ayuda a mejorar la resiliencia de las cargas de trabajo. Para obtener más información, consulte Límites de AWS aislamiento de errores.

rama de característica

Consulte la sucursal.

características

Los datos de entrada que se utilizan para hacer una predicción. Por ejemplo, en un contexto de fabricación, las características pueden ser imágenes que se capturan periódicamente desde la línea de fabricación.

importancia de las características

La importancia que tiene una característica para las predicciones de un modelo. Por lo general, se expresa como una puntuación numérica que se puede calcular mediante diversas técnicas, como las explicaciones aditivas de Shapley (SHAP) y los gradientes integrados. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con:.AWS

transformación de funciones

Optimizar los datos para el proceso de ML, lo que incluye enriquecer los datos con fuentes adicionales, escalar los valores o extraer varios conjuntos de información de un solo campo de

datos. Esto permite que el modelo de ML se beneficie de los datos. Por ejemplo, si divide la fecha del “27 de mayo de 2021 00:15:37” en “jueves”, “mayo”, “2021” y “15”, puede ayudar al algoritmo de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

FGAC

Consulte control de acceso detallado.

control de acceso detallado () FGAC

El uso de varias condiciones que tienen por objetivo permitir o denegar una solicitud de acceso.

migración relámpago

Método de migración de bases de datos que utiliza la replicación continua de datos mediante la captura de datos modificados para migrar los datos en el menor tiempo posible, en lugar de utilizar un enfoque gradual. El objetivo es reducir al mínimo el tiempo de inactividad.

G

bloqueo geográfico

Consulta las restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

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

Flujo de trabajo de Gitflow

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

estrategia de implementación desde cero

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

ampliando la infraestructura existente, puede combinar las estrategias de implementación sobre infraestructuras existentes y de implementación desde cero.

barrera de protección

Una regla de alto nivel que ayuda a regular los recursos, las políticas y el cumplimiento en todas las unidades organizativas (). OUs Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de IAM permisos. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

H

JA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

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

alta disponibilidad (HA)

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

modernización histórica

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

migración homogénea de bases de datos

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

La migración homogénea suele formar parte de un esfuerzo para volver a alojar o redefinir la plataforma. Puede utilizar las utilidades de bases de datos nativas para migrar el esquema.

datos recientes

Datos a los que se accede con frecuencia, como datos en tiempo real o datos traslacionales recientes. Por lo general, estos datos requieren un nivel o una clase de almacenamiento de alto rendimiento para proporcionar respuestas rápidas a las consultas.

hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, una revisión se suele realizar fuera del flujo de trabajo de DevOps publicación habitual.

periodo de hiperatención

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

I

IaC

Vea la infraestructura como código.

políticas basadas en identidad

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

aplicación inactiva

Aplicación que tiene un uso medio CPU de memoria entre el 5 y el 20 por ciento durante un período de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

Un modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar, aplicar parches o modificar la infraestructura existente. Las infraestructuras inmutables son intrínsecamente más consistentes, fiables y predecibles que las infraestructuras mutables. Para obtener más información, consulte las prácticas recomendadas para implementar con una infraestructura inmutable en Well-Architected Framework AWS .

entrante (ingreso) VPC

En una arquitectura AWS multicuenta, VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

migración gradual

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

Industria 4.0

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

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial () IIoT

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la

agricultura. Para obtener más información, consulte Creación de una estrategia de transformación digital del Internet de las cosas (IIoT) industrial.

inspección VPC

En una arquitectura de AWS múltiples cuentas, una arquitectura centralizada VPC que gestiona las inspecciones del tráfico de red entre Internet y las redes locales VPCs (en una misma o diferente Regiones de AWS). La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entrada, salida e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

Internet de las cosas (IoT)

Red de objetos físicos conectados con sensores o procesadores integrados que se comunican con otros dispositivos y sistemas a través de Internet o de una red de comunicación local. Para obtener más información, consulte ¿Qué es IoT?.

interpretabilidad

Característica de un modelo de machine learning que describe el grado en que un ser humano puede entender cómo las predicciones del modelo dependen de sus entradas. Para obtener más información, consulte Interpretabilidad del modelo de aprendizaje automático con. AWS

IoT

Consulte Internet de las cosas.

Biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. ITILproporciona la base paraITSM.

Administración de servicios de TI (ITSM)

Actividades asociadas con el diseño, la implementación, la administración y el soporte de los servicios de TI para una organización. Para obtener información sobre la integración de las operaciones en la nube con ITSM las herramientas, consulte la guía de integración de operaciones.

ITIL

Consulte la biblioteca de información de TI.

ITSM

Consulte Administración de servicios de TI.

L

control de acceso basado en etiquetas () LBAC

Una implementación del control de acceso obligatorio (MAC) en la que a los usuarios y a los propios datos se les asigna explícitamente un valor de etiqueta de seguridad. La intersección entre la etiqueta de seguridad del usuario y la etiqueta de seguridad de los datos determina qué filas y columnas puede ver el usuario.

zona de aterrizaje

Una landing zone es un AWS entorno multicuenta bien diseñado, escalable y seguro. Este es un punto de partida desde el cual las empresas pueden lanzar e implementar rápidamente cargas de trabajo y aplicaciones con confianza en su entorno de seguridad e infraestructura. Para obtener más información sobre las zonas de aterrizaje, consulte Configuración de un entorno de AWS seguro y escalable con varias cuentas.

migración grande

Migración de 300 servidores o más.

LBAC

Consulte el control de acceso basado en etiquetas.

privilegio mínimo

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

migrar mediante lift-and-shift

Consulte 7 Rs.

sistema little-endian

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

entornos inferiores

Véase entorno.

M

machine learning (ML)

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

rama principal

Ver sucursal.

malware

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

servicios gestionados

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

sistema de ejecución de fabricación () MES

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

cuenta de miembro

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

MES

Consulte el sistema de ejecución de la fabricación.

Transporte de telemetría y cola de mensajes () MQTT

Un protocolo de comunicación ligero machine-to-machine (M2M), basado en el patrón de publicación/suscripción, para dispositivos de IoT con recursos limitados.

microservicio

Un servicio pequeño e independiente que se comunica a través de una red bien definida APIs y que, por lo general, es propiedad de equipos pequeños e independientes. Por ejemplo, un sistema de seguros puede incluir microservicios que se adapten a las capacidades empresariales, como las de ventas o marketing, o a subdominios, como las de compras, reclamaciones o análisis. Los beneficios de los microservicios incluyen la agilidad, la escalabilidad flexible, la facilidad de implementación, el código reutilizable y la resiliencia. Para obtener más información, consulte Integrar microservicios mediante AWS servicios sin servidor.

arquitectura de microservicios

Un enfoque para crear una aplicación con componentes independientes que ejecutan cada proceso de la aplicación como un microservicio. Estos microservicios se comunican a través de una interfaz bien definida mediante un uso ligero. APIs Cada microservicio de esta arquitectura se puede actualizar, implementar y escalar para satisfacer la demanda de funciones específicas de una aplicación. Para obtener más información, consulte Implementación de microservicios en. AWS

Migration Acceleration Program (MAP)

Un AWS programa que brinda soporte de consultoría, capacitación y servicios para ayudar a las organizaciones a construir una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. MAPincluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración habituales.

migración a escala

Proceso de transferencia de la mayoría de la cartera de aplicaciones a la nube en oleadas, con más aplicaciones desplazadas a un ritmo más rápido en cada oleada. En esta fase, se utilizan las prácticas recomendadas y las lecciones aprendidas en las fases anteriores para implementar una fábrica de migración de equipos, herramientas y procesos con el fin de agilizar la migración de las cargas de trabajo mediante la automatización y la entrega ágil. Esta es la tercera fase de la estrategia de migración de AWS.

fábrica de migración

Equipos multifuncionales que agilizan la migración de las cargas de trabajo mediante enfoques automatizados y ágiles. Los equipos de las fábricas de migración suelen estar compuestos por analistas y propietarios de operaciones, ingenieros de migración, desarrolladores y DevOps profesionales que trabajan a pasos agigantados. Entre el 20 y el 50 por ciento de la cartera de aplicaciones empresariales se compone de patrones repetidos que pueden optimizarse mediante un enfoque de fábrica. Para obtener más información, consulte la discusión sobre las fábricas de migración y la Guía de fábricas de migración a la nube en este contenido.

metadatos de migración

Información sobre la aplicación y el servidor que se necesita para completar la migración. Cada patrón de migración requiere un conjunto diferente de metadatos de migración. Algunos ejemplos de metadatos de migración son la subred de destino, el grupo de seguridad y AWS la cuenta.

patrón de migración

Tarea de migración repetible que detalla la estrategia de migración, el destino de la migración y la aplicación o el servicio de migración utilizados. Ejemplo: realoje la migración a Amazon EC2 con AWS Application Migration Service.

Evaluación de la cartera de migración () MPA

Una herramienta en línea que proporciona información para validar el argumento empresarial para migrar a. Nube de AWS MPAproporciona una evaluación detallada de la cartera (tamaño correcto de los servidores, precios, TCO comparaciones y análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y planificación de la oleada). La MPAherramienta (requiere iniciar sesión) está disponible de forma gratuita para todos los consultores y AWS consultores de los socios. APN

Evaluación de la preparación para la migración (MRA)

El proceso que consiste en obtener información sobre el estado de preparación de una organización para la nube, identificar los puntos fuertes y débiles y elaborar un plan de acción para cerrar las brechas identificadas, utilizando la AWS CAF. Para obtener más información, consulte la Guía de preparación para la migración. MRAes la primera fase de la estrategia de AWS migración.

estrategia de migración

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

ML

Consulte el aprendizaje automático.

modernización

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

evaluación de la preparación para la modernización

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

aplicaciones monolíticas (monolitos)

Aplicaciones que se ejecutan como un único servicio con procesos estrechamente acoplados. Las aplicaciones monolíticas presentan varios inconvenientes. Si una característica de la aplicación experimenta un aumento en la demanda, se debe escalar toda la arquitectura. Agregar o mejorar las características de una aplicación monolítica también se vuelve más complejo a medida que crece la base de código. Para solucionar problemas con la aplicación, puede utilizar

una arquitectura de microservicios. Para obtener más información, consulte Descomposición de monolitos en microservicios.

MPA

Consulte Evaluación de la cartera de migración.

MQTT

Consulte Message Queue Queue Telemetría y Transporte.

clasificación multiclase

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

infraestructura mutable

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

O

OAC

Consulte el control de acceso de origen.

OAI

Consulte la identidad de acceso de origen.

OCM

Consulte gestión del cambio organizacional.

migración fuera de línea

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

OI

Consulte integración de operaciones.

OLA

Consulte el acuerdo a nivel operativo.

migración en línea

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

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

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

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

acuerdo a nivel operativo () OLA

Un acuerdo que aclara lo que los grupos de TI funcionales se prometen ofrecer entre sí, para respaldar un acuerdo de nivel de servicio (). SLA

revisión de la preparación operativa () ORR

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

tecnología operativa (OT)

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

integración de operaciones (OI)

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

registro de seguimiento organizativo

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

gestión del cambio organizacional (OCM)

Marco para administrar las transformaciones empresariales importantes y disruptivas desde la perspectiva de las personas, la cultura y el liderazgo. OCMayuda a las organizaciones a prepararse para los nuevos sistemas y estrategias y a realizar la transición a ellos acelerando la adopción del cambio, abordando los problemas de la transición e impulsando los cambios culturales y organizacionales. En la estrategia de AWS migración, este marco se denomina aceleración de las personas, debido a la velocidad de cambio que requieren los proyectos de adopción de la nube. Para obtener más información, consulte la OCMguía.

control de acceso de origen (OAC)

En CloudFront, una opción mejorada para restringir el acceso y proteger el contenido del Amazon Simple Storage Service (Amazon S3). OACadmite todos los depósitos de S3 Regiones de AWS, el cifrado del lado del servidor con AWS KMS (SSE-KMS) y el cifrado dinámico `PUT` y `DELETE` las solicitudes al depósito de S3.

identidad de acceso de origen () OAI

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

ORR

Consulte la revisión de la preparación operativa.

NO

Consulte tecnología operativa.

saliente (salida) VPC

En una arquitectura AWS multicuenta, VPC que gestiona las conexiones de red que se inician desde una aplicación. La arquitectura de referencia de AWS seguridad recomienda configurar

la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

P

límite de permisos

Una política IAM de administración asociada a IAM los directores para establecer los permisos máximos que puede tener el usuario o el rol. Para obtener más información, consulte los límites de los permisos en la IAM documentación.

información de identificación personal (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos PII incluyen nombres, direcciones e información de contacto.

PII

Consulte la información de identificación personal.

manual de estrategias

Conjunto de pasos predefinidos que capturan el trabajo asociado a las migraciones, como la entrega de las funciones de operaciones principales en la nube. Un manual puede adoptar la forma de scripts, manuales de procedimientos automatizados o resúmenes de los procesos o pasos necesarios para operar un entorno modernizado.

PLC

Consulte controlador lógico programable.

PLM

Consulte la gestión del ciclo de vida del producto.

política

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

persistencia políglota

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

evaluación de cartera

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

predicate

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

pulsar un predicado

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

control preventivo

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

entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz de un Cuenta de AWS, un IAM rol o un usuario. Para obtener más información, consulte los términos y conceptos de Principal in Roles en la IAM documentación.

Privacidad desde el diseño

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

zonas alojadas privadas

Un contenedor que contiene información sobre cómo desea que Amazon Route 53 responda a DNS las consultas de un dominio y sus subdominios dentro de uno o másVPCs. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

Un control de seguridad diseñado para evitar el despliegue de recursos no conformes. Estos controles escanean los recursos antes de aprovisionarlos. Si el recurso no cumple con el control, significa que no está aprovisionado. Para obtener más información, consulte la guía de referencia de controles en la AWS Control Tower documentación y consulte Controles proactivos en Implementación de controles de seguridad en AWS.

gestión del ciclo de vida del producto (PLM)

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

entorno de producción

Consulte el entorno.

controlador lógico programable () PLC

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

seudonimización

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

publicar/suscribirse (pub/sub)

Un patrón que permite las comunicaciones asíncronas entre microservicios para mejorar la escalabilidad y la capacidad de respuesta. Por ejemplo, en un microservicio basado en microservicios MES, un microservicio puede publicar mensajes de eventos en un canal al que se puedan suscribir otros microservicios. El sistema puede añadir nuevos microservicios sin cambiar el servicio de publicación.

Q

plan de consulta

Serie de pasos, como instrucciones, que se utilizan para acceder a los datos de un sistema de base de datos SQL relacional.

regresión del plan de consulta

El optimizador de servicios de la base de datos elige un plan menos óptimo que antes de un cambio determinado en el entorno de la base de datos. Los cambios en estadísticas, restricciones, configuración del entorno, enlaces de parámetros de consultas y actualizaciones del motor de base de datos PostgreSQL pueden provocar una regresión del plan.

R

RACImatriz

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

ransomware

Software malicioso que se ha diseñado para bloquear el acceso a un sistema informático o a los datos hasta que se efectúe un pago.

RASCImatriz

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

RCAC

Consulte el control de acceso por filas y columnas.

read replica

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

rediseñar

Ver 7 Rs.

objetivo de punto de recuperación (RPO)

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

objetivo de tiempo de recuperación (RTO)

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

refactorizar

Ver 7 Rs.

Región

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

regresión

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

volver a alojar

Consulte 7 Rs.

versión

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

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

resilencia

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

política basada en recursos

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

matriz responsable, responsable, consultada, informada (RACI)

Una matriz que define las funciones y responsabilidades de todas las partes involucradas en las actividades de migración y las operaciones de la nube. El nombre de la matriz se deriva de los tipos de responsabilidad definidos en la matriz: responsable (R), contable (A), consultado (C) e informado (I). El tipo de soporte (S) es opcional. Si incluye el soporte, la matriz se denomina RASCImatriz y, si la excluye, se denomina RACImatriz.

control receptivo

Un control de seguridad que se ha diseñado para corregir los eventos adversos o las desviaciones con respecto a su base de seguridad. Para obtener más información, consulte Controles receptivos en Implementación de controles de seguridad en AWS.

retain

Consulte 7 Rs.

jubilarse

Ver 7 Rs.

rotación

Proceso de actualizar periódicamente un secreto para dificultar el acceso de un atacante a las credenciales.

control de acceso por filas y columnas (RCAC)

El uso de SQL expresiones básicas y flexibles que tienen reglas de acceso definidas. RCACconsta de permisos de fila y máscaras de columnas.

RPO

Consulte el objetivo del punto de recuperación.

RTO

Consulte el objetivo de tiempo de recuperación.

manual de procedimientos

Conjunto de procedimientos manuales o automatizados necesarios para realizar una tarea específica. Por lo general, se diseñan para agilizar las operaciones o los procedimientos repetitivos con altas tasas de error.

S

SAML2.0

Un estándar abierto que utilizan muchos proveedores de identidad (IdPs). Esta función permite el inicio de sesión único (SSO) federado, de modo que los usuarios pueden iniciar sesión AWS Management Console o llamar a las AWS API operaciones sin tener que crear un registro de usuario IAM para todos los miembros de la organización. Para obtener más información sobre la federación SAML basada en 2.0, consulte Acerca de la federación basada SAML en 2.0 en la documentación. IAM

SCADA

Consulte el control de supervisión y la adquisición de datos.

SCP

Consulte la política de control de servicios.

secreta

Información confidencial o restringida, como una contraseña o credenciales de usuario, que almacene de forma cifrada. AWS Secrets Manager Se compone del valor secreto y sus metadatos. El valor secreto puede ser binario, una sola cadena o varias cadenas. Para obtener más información, consulta ¿Qué hay en un secreto de Secrets Manager? en la documentación de Secrets Manager.

control de seguridad

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

refuerzo de la seguridad

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

sistema de información de seguridad y gestión de eventos (SIEM)

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

automatización de las respuestas de seguridad

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

cifrado del servidor

Cifrado de los datos en su destino, por parte de Servicio de AWS quien los recibe.

política de control de servicios (SCP)

Una política que proporciona un control centralizado de los permisos de todas las cuentas de una organización en AWS Organizations. SCPsdefina barreras o establezca límites a las acciones que un administrador puede delegar en usuarios o roles. Puede utilizarlas SCPs como listas de permitidos o rechazados para especificar qué servicios o acciones están permitidos o prohibidos. Para obtener más información, consulte las políticas de control de servicios en la AWS Organizations documentación.

punto de enlace de servicio

El URL del punto de entrada de un Servicio de AWS. Para conectarse mediante programación a un servicio de destino, puede utilizar un punto de conexión. Para obtener más información, consulte Puntos de conexión de Servicio de AWS en Referencia general de AWS.

acuerdo de nivel de servicio () SLA

Acuerdo que aclara lo que un equipo de TI se compromete a ofrecer a los clientes, como el tiempo de actividad y el rendimiento del servicio.

indicador de nivel de servicio () SLI

Medición de un aspecto del rendimiento de un servicio, como la tasa de errores, la disponibilidad o el rendimiento.

objetivo de nivel de servicio () SLO

Una métrica objetivo que representa el estado de un servicio, medido mediante un indicador de nivel de servicio.

modelo de responsabilidad compartida

Un modelo que describe la responsabilidad que compartes con respecto a la seguridad y AWS el cumplimiento de la nube. AWS es responsable de la seguridad de la nube, mientras que usted es responsable de la seguridad en la nube. Para obtener más información, consulte el Modelo de responsabilidad compartida.

SIEM

Consulte la información de seguridad y el sistema de gestión de eventos.

punto único de fallo (SPOF)

Una falla en un único componente crítico de una aplicación que puede interrumpir el sistema.

SLA

Consulte el acuerdo de nivel de servicio.

SLI

Consulte el indicador de nivel de servicio.

SLO

Consulte el objetivo de nivel de servicio.

split-and-seed modelo

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

SPOF

Consulte el punto único de fallo.

esquema en forma de estrella

Estructura organizativa de una base de datos que utiliza una tabla de 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 de cómo aplicar este patrón, consulta Modernizar la versión antigua de MicrosoftASP. NET(ASMX) servicios web de forma incremental mediante contenedores y Amazon API Gateway.

subred

Un rango de direcciones IP en su. VPC Una subred debe residir en una sola zona de disponibilidad.

control de supervisión y adquisición de datos (SCADA)

En la industria manufacturera, un sistema que utiliza hardware y software para monitorear los activos físicos y las operaciones de producción.

cifrado simétrico

Un algoritmo de cifrado que utiliza la misma clave para cifrar y descifrar los datos.

pruebas sintéticas

Probar un sistema de manera que simule las interacciones de los usuarios para detectar posibles problemas o monitorear el rendimiento. Puede usar Amazon CloudWatch Synthetics para crear estas pruebas.

T

etiquetas

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS Las etiquetas pueden ayudarle a administrar, identificar, organizar, buscar y filtrar recursos. Para obtener más información, consulte Etiquetado de los recursos de AWS.

variable de destino

El valor que intenta predecir en el ML supervisado. Esto también se conoce como variable de resultado. Por ejemplo, en un entorno de fabricación, la variable objetivo podría ser un defecto del producto.

lista de tareas

Herramienta que se utiliza para hacer un seguimiento del progreso mediante un manual de procedimientos. La lista de tareas contiene una descripción general del manual de procedimientos y una lista de las tareas generales que deben completarse. Para cada tarea general, se incluye la cantidad estimada de tiempo necesario, el propietario y el progreso.

entorno de prueba

Consulte entorno.

entrenamiento

Proporcionar datos de los que pueda aprender su modelo de ML. Los datos de entrenamiento deben contener la respuesta correcta. El algoritmo de aprendizaje encuentra patrones en los datos de entrenamiento que asignan los atributos de los datos de entrada al destino (la respuesta que desea predecir). Genera un modelo de ML que captura estos patrones. Luego, el modelo de ML se puede utilizar para obtener predicciones sobre datos nuevos para los que no se conoce el destino.

puerta de enlace de tránsito

Un centro de tránsito de red que puede usar para interconectar sus VPCs redes con las locales. Para obtener más información, consulte Qué es una pasarela de tránsito en la AWS Transit Gateway documentación.

flujo de trabajo basado en enlaces troncales

Un enfoque en el que los desarrolladores crean y prueban características de forma local en una rama de característica y, a continuación, combinan esos cambios en la rama principal. Luego, la rama principal se adapta a los entornos de desarrollo, preproducción y producción, de forma secuencial.

acceso de confianza

Otorgar permisos a un servicio que especifique para realizar tareas en su organización AWS Organizations y en sus cuentas en su nombre. El servicio de confianza crea un rol vinculado al servicio en cada cuenta, cuando ese rol es necesario, para realizar las tareas de administración por usted. Para obtener más información, consulte AWS Organizations Utilización con otros AWS servicios en la AWS Organizations documentación.

ajuste

Cambiar aspectos de su proceso de formación a fin de mejorar la precisión del modelo de ML. Por ejemplo, puede entrenar el modelo de ML al generar un conjunto de etiquetas, incorporar etiquetas y, luego, repetir estos pasos varias veces con diferentes ajustes para optimizar el modelo.

equipo de dos pizzas

Un DevOps equipo pequeño al que puedes alimentar con dos pizzas. Un equipo formado por dos integrantes garantiza la mejor oportunidad posible de colaboración en el desarrollo de software.

U

incertidumbre

Un concepto que hace referencia a información imprecisa, incompleta o desconocida que puede socavar la fiabilidad de los modelos predictivos de ML. Hay dos tipos de incertidumbre: la incertidumbre epistémica se debe a datos limitados e incompletos, mientras que la incertidumbre aleatoria se debe al ruido y la aleatoriedad inherentes a los datos. Para más información, consulte la guía Cuantificación de la incertidumbre en los sistemas de aprendizaje profundo.

tareas indiferenciadas

También conocido como tareas arduas, es el trabajo que es necesario para crear y operar una aplicación, pero que no proporciona un valor directo al usuario final ni proporciona una ventaja competitiva. Algunos ejemplos de tareas indiferenciadas son la adquisición, el mantenimiento y la planificación de la capacidad.

entornos superiores

Ver entorno.

V

succión

Una operación de mantenimiento de bases de datos que implica limpiar después de las actualizaciones incrementales para recuperar espacio de almacenamiento y mejorar el rendimiento.

control de versión

Procesos y herramientas que realizan un seguimiento de los cambios, como los cambios en el código fuente de un repositorio.

VPCmirando

Una conexión entre dos VPCs que permite enrutar el tráfico mediante direcciones IP privadas. Para obtener más información, consulta Qué es el VPC peering en la VPC documentación de Amazon.

vulnerabilidad

Defecto de software o hardware que pone en peligro la seguridad del sistema.

W

caché caliente

Un búfer caché que contiene datos actuales y relevantes a los que se accede con frecuencia. La instancia de base de datos puede leer desde la caché del búfer, lo que es más rápido que leer desde la memoria principal o el disco.

datos templados

Datos a los que el acceso es infrecuente. Al consultar este tipo de datos, normalmente se aceptan consultas moderadamente lentas.

función de ventana

SQLFunción que realiza un cálculo en un grupo de filas que se relacionan de alguna manera con el registro actual. Las funciones de ventana son útiles para procesar tareas, como calcular una media móvil o acceder al valor de las filas en función de la posición relativa de la fila actual.

carga de trabajo

Conjunto de recursos y código que ofrece valor comercial, como una aplicación orientada al cliente o un proceso de backend.

flujo de trabajo

Grupos funcionales de un proyecto de migración que son responsables de un conjunto específico de tareas. Cada flujo de trabajo es independiente, pero respalda a los demás flujos de trabajo del proyecto. Por ejemplo, el flujo de trabajo de la cartera es responsable de priorizar las aplicaciones, planificar las oleadas y recopilar los metadatos de migración. El flujo de trabajo de la cartera entrega estos recursos al flujo de trabajo de migración, que luego migra los servidores y las aplicaciones.

WORM

Mira, escribe una vez, lee muchas.

WQF

Consulte el marco AWS de calificación de la carga de trabajo.

escribe una vez, lee muchas (WORM)

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

Z

ataque de día cero

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

vulnerabilidad de día cero

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

aplicación zombi

Una aplicación que tiene un uso medio CPU de memoria inferior al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.