AWS Arquitectura de referencia de privacidad (AWS PRA)

AWS Guía prescriptiva

AWS Guía prescriptiva: AWS Arquitectura de referencia de privacidad (AWS PRA)

Table of Contents

AWS Arquitectura de referencia de privacidad (AWS PRA)

Amazon Web Services (colaboradores)

Marzo de 2024 (historial del documento)

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

Avisos

Esta guía se proporciona únicamente con fines informativos. No es asesoramiento legal y no debe considerarse asesoramiento legal. AWS alienta a sus clientes a obtener el asesoramiento adecuado sobre la implementación de los entornos de privacidad y protección de datos y, de manera más general, de las leyes aplicables relevantes a sus negocios.

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. Este documento: (a) tiene únicamente fines informativos, (b) representa las ofertas y prácticas de AWS productos actuales, que están sujetas a cambios sin previo aviso, y (c) no implica ningún compromiso ni garantía por parte de AWS sus filiales, proveedores o licenciantes. AWS los productos o servicios se proporcionan «tal cual» sin garantías, representaciones o condiciones de ningún tipo, ya sean expresas o implícitas.

Las responsabilidades y obligaciones de AWS sus clientes están reguladas por AWS acuerdos, y este documento no forma parte de ningún acuerdo entre sus clientes AWS y sus clientes ni lo modifica.

Introducción

La arquitectura AWS de referencia de privacidad (PRA) proporciona un conjunto de pautas específicas para el diseño y la configuración de los controles que respaldan la privacidad en. Servicios de AWS Esta guía puede ayudarlo a tomar decisiones sobre las personas, los procesos y la tecnología que ayudan a respaldar la privacidad en el mundo. Nube de AWS

El modelo de responsabilidad AWS compartida y la privacidad

En el Nube de AWS, usted comparte la responsabilidad de la seguridad y el cumplimiento de AWS. AWS es responsable de la seguridad de la nube, lo que significa que AWS es responsable de proteger la infraestructura en la que se ejecutan todos los servicios que se ofrecen en la nube Nube de AWS. Usted es responsable de la seguridad en la nube, lo que significa que es responsable de configurarla y administrarla Servicios de AWS de acuerdo con los requisitos de seguridad y privacidad. Para obtener más información, consulte el modelo de responsabilidad AWS compartida.

Servicios de AWS proporcionan capacidades que le permiten implementar sus propios controles de privacidad en la nube para cumplir con sus requisitos de privacidad. Su responsabilidad en materia de privacidad varía en función de muchos factores, como la Servicios de AWS forma en Regiones de AWS que usted elija, la integración de esos servicios en su entorno de TI y las leyes y reglamentos aplicables a su organización y carga de trabajo.

Al usarlos Servicios de AWS, mantienes el control sobre tu contenido. En concreto, el contenido se define como el software (incluidas las imágenes de las máquinas), los datos, el texto, el audio, el vídeo o las imágenes que usted o cualquier usuario final nos transfiere para su procesamiento, almacenamiento o alojamiento Servicios de AWS en relación con su cuenta. También incluye cualquier resultado computacional que usted o un usuario final obtengan mediante su uso Servicios de AWS. Usted es responsable de gestionar las siguientes decisiones, que están bajo su control:

- Los datos que decide recopilar, almacenar o procesar AWS
- Los Servicios de AWS que usa con los datos
- El Región de AWS lugar donde recopila, almacena o procesa los datos
- El formato y la estructura de sus datos y si están enmascarados, anonimizados o cifrados
- Cómo se definen, almacenan, rotan y utilizan las claves criptográficas para el cifrado
- Quién tiene acceso y cuándo tiene acceso a sus datos, y cómo se otorgan, administran y revocan esos derechos de acceso

Una vez que comprenda el modelo de responsabilidad AWS compartida y cómo se aplica generalmente al funcionamiento en la nube, debe determinar cómo se aplica a su caso de uso. La configuración Servicios de AWS que elija utilizar determinará la cantidad de configuración que debe realizar como parte de las responsabilidades de privacidad de su organización. Por ejemplo, un servicio como Amazon Elastic Compute Cloud (Amazon EC2) se clasifica como infraestructura como servicio (IaaS). Por lo tanto, si utilizas Amazon EC2, debes realizar todas las configuraciones de

privacidad necesarias para los sistemas operativos invitados y para el software de aplicación o las utilidades que instales en tus EC2 instancias. Cuando utiliza un servicio abstracto, como Amazon Simple Storage Service (Amazon S3) y Amazon DynamoDB AWS , es responsable de la capa de infraestructura, el sistema operativo y las plataformas. Su responsabilidad consiste en gestionar y clasificar los datos y configurar las políticas utilizadas para acceder a los puntos finales con el fin de almacenar y recuperar datos. Para obtener más información sobre cómo lo AWS ayuda a proteger los datos y la privacidad, consulte Protección de datos y privacidad en AWS.

Entendiendo la AWS PRA

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

En esta sección se describe la relación entre la arquitectura AWS de referencia de privacidad (AWS PRA) y otras AWS directrices. En esta sección también se analizan el diseño y la estructura generales del ejemplo de entorno de AWS cuentas múltiples de la AWS PRA.

Esta sección contiene los siguientes temas:

- Uso de la AWS PRA y la SRA AWS
- AWS Organizations y la estructura contable dedicada
- Operacionalizar AWS los servicios de privacidad

Uso de la AWS PRA y la SRA AWS

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

La AWS PRA proporciona patrones que los clientes han considerado útiles a la hora de planificar los controles de privacidad fundamentales y a nivel de aplicación para su infraestructura y sus cargas de trabajo. AWS La arquitectura de referencia de AWS seguridad (AWS SRA) proporciona un conjunto de pautas para crear una arquitectura que implemente y respalde el conjunto correcto de controles de seguridad en tu AWS landing zone y tus aplicaciones. Para establecer los controles de privacidad detallados en esta guía, la AWS PRA parte de muchas de las mismas directrices fundamentales y de la misma estructura contable que se describen en la AWS SRA. La AWS PRA y la AWS SRA detallan muchas de las mismas claves. Servicios de AWS Esta guía incluye solo descripciones breves de estos servicios. Puede obtener más información sobre estos servicios y cómo se utilizan en un contexto de seguridad en la AWS SRA.

La AWS SRA puede ayudarlo a diseñar, implementar y administrar los servicios de AWS seguridad para que se ajusten a las prácticas AWS recomendadas. Puede utilizar la AWS SRA como guía

independiente, o puede utilizar la AWS SRA y la AWS PRA como guías complementarias. Muchas de las pautas de seguridad detalladas en la AWS SRA se pueden seguir junto con los controles de privacidad que se detallan en la PRA. AWS Al igual que en el caso de la seguridad, hay algunas consideraciones fundamentales sobre la privacidad que puede ser útil tener en cuenta al principio del Nube de AWS proceso, ya que estas decisiones pueden afectar al diseño de la estructura contable de la organización. Por ejemplo, algunas de las preguntas que podrías plantearte son las siguientes:

- ¿Cómo define mi organización los datos personales?
- ¿Mi organización admite las aplicaciones que procesan datos personales?
- ¿Qué pasa con las aplicaciones que procesan otros tipos de datos regulados?
- ¿Qué controles a nivel organizativo puedo implementar para mantener a mis desarrolladores e ingenieros de nube lo más alejados posible de los datos personales?
- ¿Cómo puedo separar los datos personales de otros tipos de datos?
- ¿Cuáles son los requisitos de transferencia de datos transfronteriza de mi organización?

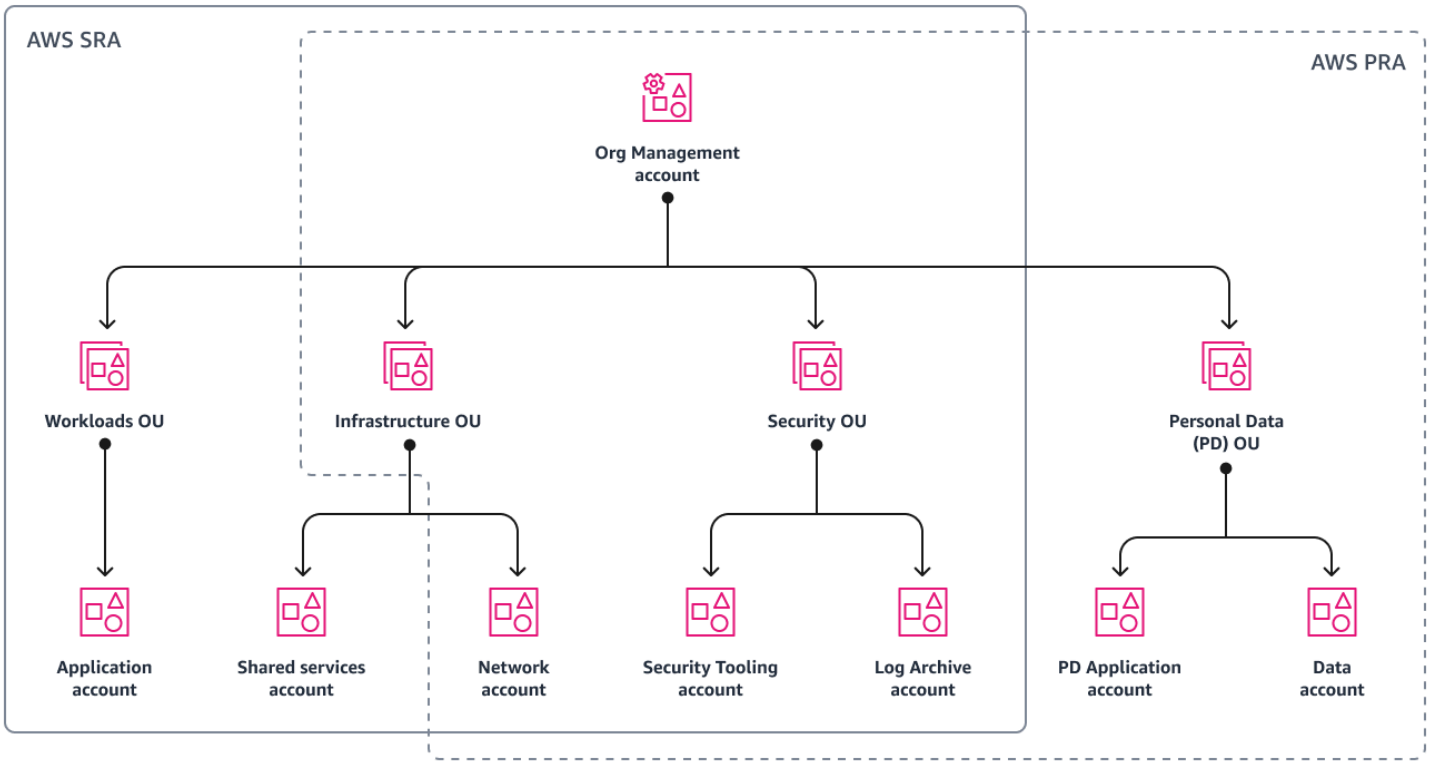
Las respuestas a muchas de estas preguntas pueden tener implicaciones en el diseño de su entorno de nube, como su Cuenta de AWS estructura, las políticas de control de servicios y las funciones AWS Identity and Access Management (IAM).

AWS Organizations y la estructura contable dedicada

> Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

AWS Organizationses un servicio de administración de cuentas que le ayuda a gestionar y gestionar múltiples cuentas de forma centralizada Cuentas de AWS. El uso de AWS Organizations es la base de un entorno de múltiples AWS cuentas bien diseñado. Para obtener más información, consulte Establecer un entorno de mejores prácticas. AWS

El siguiente diagrama muestra la estructura de cuentas y unidades organizativas (OU) de alto nivel de la AWS PRA. En su mayor parte, la estructura organizativa de la AWS PRA coincide con la estructura organizativa de la AWS SRA.



Las desviaciones con respecto a la organización de la AWS SRA incluyen:

- La AWS PRA añade la OU de datos personales (PD), que se dedica a recopilar, almacenar y procesar datos personales. Esta separación estructural proporciona flexibilidad para que pueda definir controles específicos y detallados que ayuden a proteger los datos personales de la divulgación no intencionada.
- En la OU de infraestructura, la AWS PRA no incluye actualmente directrices adicionales para la cuenta de servicios compartidos que se describen en la SRA. AWS
- Actualmente, la AWS PRA no incluye directrices adicionales para la OU de cargas de trabajo que se describen en la AWS SRA. Las aplicaciones que recopilan o procesan datos personales se encuentran en cuentas específicas en la PD OU.

Puede utilizarlas AWS Control Towerpara una gobernanza básica general y para el despliegue automatizado de los controles de seguridad y privacidad en toda su organización. Si su organización AWS Control Tower no los utiliza actualmente, puede implementar muchos de los controles de seguridad y privacidad AWS Control Tower, como las políticas y AWS Config reglas de control de servicios, en sus respectivos servicios.

Puede que le resulte útil tener en cuenta el procesamiento de los datos personales al planificar la estructura de su cuenta y unidad organizativa, incluida una estrategia de segmentación de cuentas. Es posible que tengas que tener en cuenta los tipos de datos que estás procesando en función de sus casos de uso específicos y de las leyes y reglamentos aplicables. Por ejemplo, los datos del titular de la tarjeta están protegidos por el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS), y la información de salud protegida puede estar sujeta a la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA). Es posible que desee revisar qué entornos contienen datos personales y planificar su estrategia de segmentación en función de ello. Una estrategia de segmentación de cuentas típica puede incluir cuentas específicas Cuentas de AWS que se adapten al ciclo de vida del desarrollo del software (SDLC), como cuentas dedicadas al desarrollo, la preparación o el control de calidad (QA) y la producción. Una estrategia de segmentación como esta puede ser un componente fundamental en el debate general sobre el diseño, y es OUs posible que deba ajustarse a sus requisitos reglamentarios específicos.

Operacionalizar AWS los servicios de privacidad

> Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

Para muchos, la privacidad es transversal. Muchos equipos diferentes tienen un papel que desempeñar, incluidos los equipos de regulación, cumplimiento e ingeniería. Cuando su organización haya empezado a definir las personas y los componentes políticos clave de su programa de privacidad, podrá asignar los controles a un marco de cumplimiento de la privacidad para lograr operaciones coherentes. Un marco puede servir como rúbrica para implementar controles de privacidad básicos y específicos de cada aplicación para los datos personales en su entorno. AWS

Independientemente del marco que utilicen los clientes para clasificar sus requisitos de privacidad, los equipos de cumplimiento, ingeniería de privacidad y aplicaciones suelen tener que trabajar juntos para alcanzar los objetivos de implementación. Por ejemplo, los equipos de regulación y cumplimiento pueden proporcionar los requisitos de alto nivel, y los equipos de ingeniería y aplicaciones pueden configurar Servicios de AWS y utilizar las funciones para adaptarlos a estos requisitos. Empezar con un marco de control puede ayudarle a definir controles organizativos y técnicos más prescriptivos.

Al definir los controles técnicos Servicios de AWS y las características, otra decisión clave es si el control debe aplicarse a toda la organización, a una unidad organizativa, a una cuenta o a un recurso

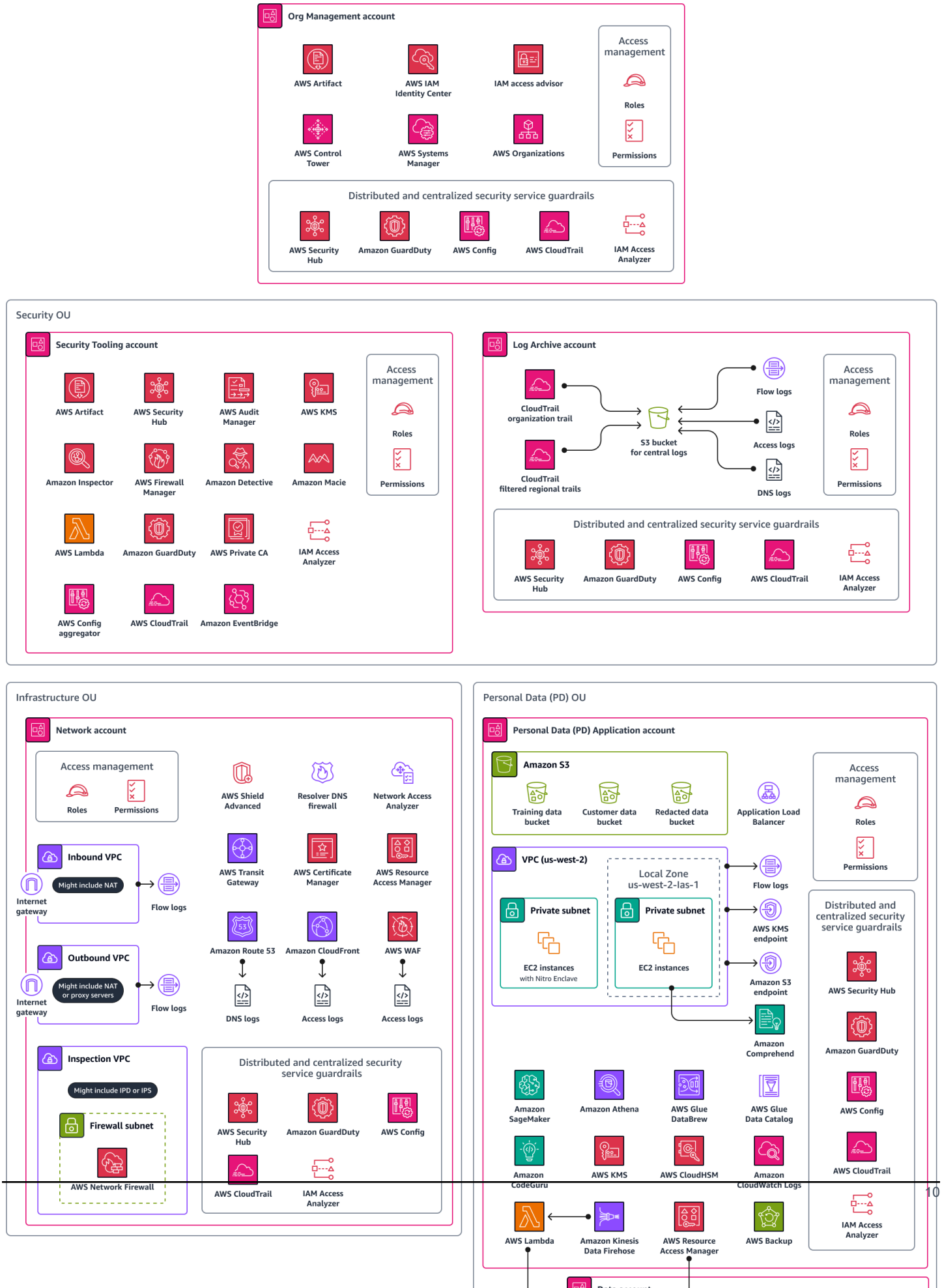
específico. Algunos servicios y funciones son ideales para implementar controles en toda AWS la organización. Por ejemplo, bloquear el acceso público a los buckets de Amazon S3 es un control específico que se configura preferiblemente en la raíz de la organización y no de forma individual para cada cuenta. Sin embargo, sus políticas de retención pueden variar de una aplicación a otra, lo que significa que puede aplicar el control a nivel de recursos.

Para ayudarlo a acelerar la operacionalización de la privacidad en su organización, AWS ofrece servicios de asesoría de auditoría y cumplimiento para sus cargas de AWS trabajo. Para obtener más información, póngase en contacto con SAS AWS.

La arquitectura AWS de referencia de privacidad

Nos encantaría saber de usted. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

El siguiente diagrama ilustra la arquitectura AWS de referencia de privacidad (AWS PRA). Este es un ejemplo de una arquitectura que conecta muchas funciones y funciones relacionadas con la privacidad Servicios de AWS . Esta arquitectura se basa en una zona de aterrizaje que se rige por AWS Control Tower.


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
AWS Control Tower
AWS Systems Manager
AWS Organizations
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Security OU
Security Tooling account
AWS Artifact
AWS Security Hub
AWS Audit Manager
AWS KMS
Amazon Inspector
AWS Firewall Manager
Amazon Detective
Amazon Macie
AWS Lambda
Amazon GuardDuty
AWS Private CA
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Access management
Roles
Permissions
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Infrastructure OU
Network account
Access management
Roles
Permissions
Inbound VPC
Might include NAT
Internet gateway
Flow logs
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Personal Data (PD) OU
Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application Load Balancer
VPC (us-west-2)
Local Zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Amazon Comprehend
Access management
Roles
Permissions
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon SageMaker
Amazon Athena
AWS Glue DataBrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup

La AWS PRA incluye una arquitectura web sin servidor que se aloja en la cuenta de la aplicación de datos personales (PD). La arquitectura de esta cuenta es un ejemplo de carga de trabajo que recopila datos personales directamente de los consumidores. En esta carga de trabajo, los usuarios se conectan a través de un nivel web. El nivel web interactúa con el nivel de aplicación. Este nivel recibe información del nivel web, procesa y almacena los datos, permite que los equipos internos autorizados y terceros accedan a los datos y, finalmente, los archiva y elimina cuando ya no son necesarios. La arquitectura es modular a propósito y se basa en eventos para demostrar muchas de las técnicas fundamentales de ingeniería de privacidad sin profundizar en casos de uso específicos, como lagos de datos, contenedores, computación o Internet de las cosas (IoT).

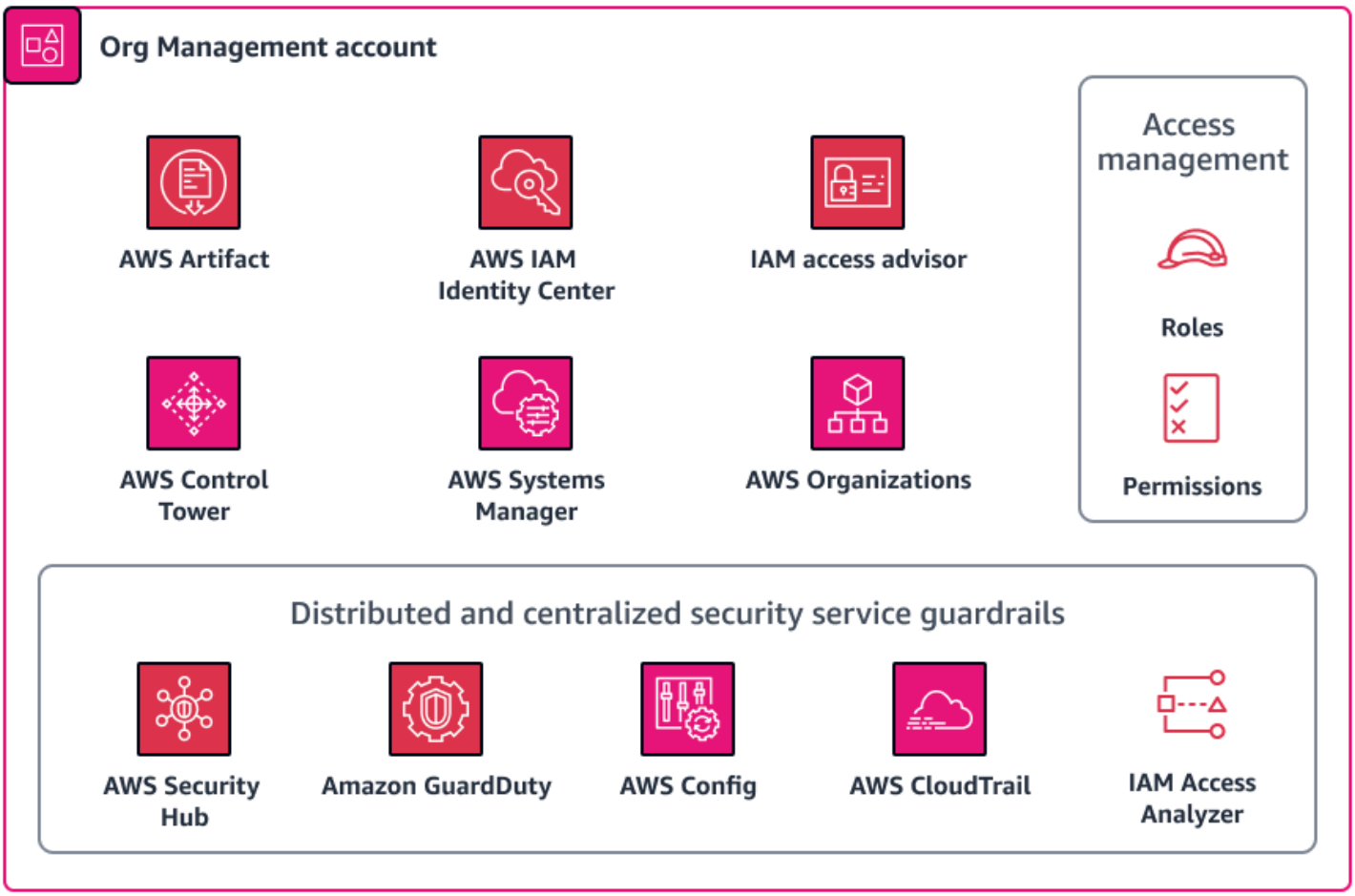
A continuación, en esta guía se describe en detalle cada cuenta de la organización. En ella se analizan los servicios y las características relacionados con la privacidad, las consideraciones y recomendaciones, y los diagramas de cada una de las siguientes cuentas:

- Cuenta de administración de la organización
- Security OU: cuenta de herramientas de seguridad
- Cuenta Security OU — Log Archive
- Unidad organizativa de infraestructura: cuenta de red
- Datos personales: OU: cuenta de aplicación PDF

Cuenta de administración de la organización

> Nos encantaría saber de usted. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

La cuenta de administración de la organización se utiliza principalmente para gestionar los cambios en la configuración de los recursos para los controles de privacidad fundamentales en todas las cuentas de su organización, que está gestionada por AWS Organizations. En esta cuenta también puede implementar nuevas cuentas de miembros de forma coherente, con muchos de los mismos controles de seguridad y privacidad. Para obtener más información sobre esta cuenta, consulte la Arquitectura AWS de referencia de seguridad (AWS SRA). El siguiente diagrama ilustra los servicios de AWS seguridad y privacidad que están configurados en la cuenta de administración de la organización.



En esta sección se proporciona información más detallada sobre lo siguiente Servicios de AWS que se utiliza en esta cuenta:

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifactpuede ayudarlo con las auditorías al proporcionar descargas a pedido de documentos de AWS seguridad y cumplimiento. Para obtener más información sobre cómo se utiliza este servicio en un contexto de seguridad, consulte la arquitectura AWS de referencia de seguridad.

Esto le Servicio de AWS ayuda a comprender los controles que hereda AWS y a determinar qué controles le quedan por implementar en su entorno. AWS Artifact proporciona acceso a los informes AWS de seguridad y conformidad, como los informes de controles de sistemas y organizaciones

(SOC) y los informes del sector de las tarjetas de pago (PCI). También proporciona acceso a las certificaciones de los organismos de acreditación de diferentes regiones geográficas y verticales de cumplimiento que validan la implementación y la eficacia operativa de los controles. AWS Si lo utiliza AWS Artifact, puede proporcionar los artefactos de AWS auditoría a sus auditores o reguladores como prueba de los controles de AWS seguridad. Los siguientes informes pueden resultar útiles para demostrar la eficacia de los controles de AWS privacidad:

- Informe de privacidad tipo 2 del SOC 2: este informe demuestra la eficacia de AWS los controles sobre la forma en que se recopilan, utilizan, retienen, divulgan y eliminan los datos personales. Para obtener más información, consulta las preguntas frecuentes sobre el SOC.
- Informe de privacidad del SOC 3: el informe de privacidad del SOC 3 es una descripción menos detallada de los controles de privacidad del SOC, de circulación general.
- Informe de certificación ISO/IEC 27701:2019: la norma ISO/IEC 27701:2019 describe los requisitos y directrices para establecer y mejorar continuamente un sistema de gestión de la información de privacidad (PIMS). Este informe detalla el alcance de esta certificación y puede servir como prueba de certificación. AWS Para obtener más información sobre esta norma, consulte la norma ISO/IEC 27701:2019 (sitio web de la ISO).

AWS Control Tower

AWS Control Towerle ayuda a configurar y administrar un entorno de AWS múltiples cuentas que sigue las mejores prácticas de seguridad prescriptivas. Para obtener más información sobre cómo se utiliza este servicio en un contexto de seguridad, consulte la Arquitectura de referencia AWS de seguridad.

También puede automatizar la implementación de una serie de controles proactivos, preventivos y de detección, también conocidos como barreras de protección, que se adaptan a sus requisitos de residencia y protección de datos. AWS Control Tower Por ejemplo, puede especificar barreras que limiten la transferencia de datos solo a los aprobados. Regiones de AWS Para un control aún más detallado, puede elegir entre más de 17 barandas diseñadas para controlar la residencia de los datos, como no permitir las conexiones de la Red Privada Virtual (VPN) de Amazon, No permitir el acceso a Internet para una instancia de Amazon VPC y Denegar el acceso a AWS según lo solicitado. Región de AWS Estas barreras se componen de una serie de AWS CloudFormation enlaces, políticas de control de servicios y AWS Config reglas que se pueden implementar de manera uniforme en toda la organización. Para obtener más información, consulte los controles que mejoran la protección de la residencia de los datos en la documentación. AWS Control Tower

Si necesita implementar barreras de privacidad más allá de los controles de residencia de datos, AWS Control Tower incluye una serie de controles obligatorios. Estos controles se despliegan de forma predeterminada en todas las unidades organizativas cuando configuras tu landing zone. Muchos de estos son controles preventivos diseñados para proteger los registros, como prohibir la eliminación del archivo de registros y habilitar la validación de integridad del archivo de CloudTrail registro.

AWS Control Tower también está integrado AWS Security Hub para proporcionar controles de detección. Estos controles se conocen como estándar gestionado por el servicio:. AWS Control Tower Puede utilizar estos controles para supervisar los cambios en la configuración de los controles que respaldan la privacidad, como el cifrado en reposo para las instancias de bases de datos de Amazon Relational Database Service (Amazon RDS).

AWS Organizations

El AWS PRA se utiliza AWS Organizations para gestionar de forma centralizada todas las cuentas de la arquitectura. Para obtener más información, consulte la sección AWS Organizations y la estructura contable dedicada de esta guía. En AWS Organizations, puede utilizar las políticas de control de servicios (SCPs) y las políticas de administración para ayudar a proteger los datos personales y la privacidad.

Políticas de control de servicios (SCPs)

Las políticas de control de servicios (SCPs) son un tipo de política organizacional que puede usar para administrar los permisos en su organización. Proporcionan un control centralizado sobre los permisos máximos disponibles para los roles y usuarios AWS Identity and Access Management (IAM) en la cuenta de destino, la unidad organizativa (OU) o toda la organización. Puede crearlos y solicitarlos SCPs desde la cuenta de administración de la organización.

Puede utilizarla AWS Control Tower para realizar una implementación SCPs uniforme en todas sus cuentas. Para obtener más información sobre los controles de residencia de datos que puede aplicar AWS Control Tower, consulte AWS Control Tower esta guía. AWS Control Tower incluye un complemento completo de medidas preventivas. SCPs Si AWS Control Tower no se utiliza actualmente en su organización, también puede implementar estos controles manualmente.

Se utiliza SCPs para cumplir con los requisitos de residencia de los datos

Es habitual gestionar los requisitos de residencia de los datos personales almacenando y procesando los datos dentro de una región geográfica específica. Para verificar que se cumplen los requisitos de residencia de datos exclusivos de una jurisdicción, le recomendamos que colabore

estrechamente con su equipo regulador para confirmar sus requisitos. Cuando se hayan determinado estos requisitos, hay una serie de controles de privacidad AWS fundamentales que pueden ayudar a respaldarlos. Por ejemplo, se pueden utilizar SCPs para limitar cuáles se Regiones de AWS pueden utilizar para procesar y almacenar datos. Para ver un ejemplo de política, consulta Restrinja las transferencias de datos entre Regiones de AWS esta guía.

Se usa SCPs para restringir las llamadas a la API de alto riesgo

Es importante entender de qué controles de seguridad y privacidad AWS es responsable y de cuáles es responsable usted. Por ejemplo, eres responsable de los resultados de las llamadas a la API que se puedan realizar con la Servicios de AWS que utilizas. También es responsable de comprender cuáles de esas llamadas podrían provocar cambios en su postura en materia de seguridad o privacidad. Si te preocupa mantener una determinada postura de seguridad y privacidad, puedes habilitar SCPs esa opción para denegar determinadas llamadas a la API. Estas llamadas a la API pueden tener implicaciones, como la divulgación no intencionada de datos personales o la violación de determinadas transferencias transfronterizas de datos. Por ejemplo, es posible que desees prohibir las siguientes llamadas a la API:

- Habilitar el acceso público a los depósitos de Amazon Simple Storage Service (Amazon S3)
- Desactivar Amazon GuardDuty o crear reglas de supresión para los hallazgos de exfiltración de datos, como el hallazgo Trojan: EC2 /Exfiltration DNSData
- Eliminar las reglas de exfiltración de datos AWS WAF
- Compartir públicamente las instantáneas de Amazon Elastic Block Store (Amazon EBS)
- Eliminar una cuenta de miembro de la organización
- Desasociar Amazon CodeGuru Reviewer de un repositorio

Políticas de administración

Las políticas de administración AWS Organizations pueden ayudarle a configurar Servicios de AWS y gestionar sus funciones de forma centralizada. Los tipos de políticas de administración que elija determinan cómo afectan las políticas a las cuentas que las heredan OUs y a las cuentas que las heredan. Las políticas de etiquetas son un ejemplo de política de administración AWS Organizations que se relaciona directamente con la privacidad.

Uso de políticas de etiquetas

Las etiquetas son pares de valores clave que ayudan a administrar, identificar, organizar, buscar y filtrar AWS los recursos. Puede resultar útil aplicar etiquetas que distingan los recursos de la

organización que gestionan datos personales. El uso de etiquetas es compatible con muchas de las soluciones de privacidad de esta guía. Por ejemplo, es posible que desee aplicar una etiqueta que indique la clasificación general de los datos que se procesan o almacenan en el recurso. Puede escribir políticas de control de acceso basadas en atributos (ABAC) que limiten el acceso a los recursos que tienen una etiqueta o un conjunto de etiquetas en particular. Por ejemplo, tu política puede especificar que el `SysAdmin` rol no puede acceder a los recursos que tienen la etiqueta. `dataclassification:4` Para obtener más información y un tutorial, consulte Definir los permisos de acceso a AWS los recursos en función de las etiquetas en la documentación de IAM. Además, si su organización suele AWS Backupaplicar políticas de retención de datos de manera amplia en las copias de seguridad de muchas cuentas, puede aplicar una etiqueta que sitúe ese recurso dentro del ámbito de aplicación de esa política de copias de seguridad.

Las políticas de etiquetas le ayudan a mantener etiquetas coherentes en toda la organización. En una política de etiquetas, se especifican las reglas que se aplican a los recursos cuando se etiquetan. Por ejemplo, puede requerir que los recursos se etiqueten con claves específicas, como `DataClassification` o`DataSteward`, y puede especificar valores o tratamientos de mayúsculas y minúsculas válidos para las claves. También puede utilizar la aplicación para evitar que se completen las solicitudes de etiquetado no conformes.

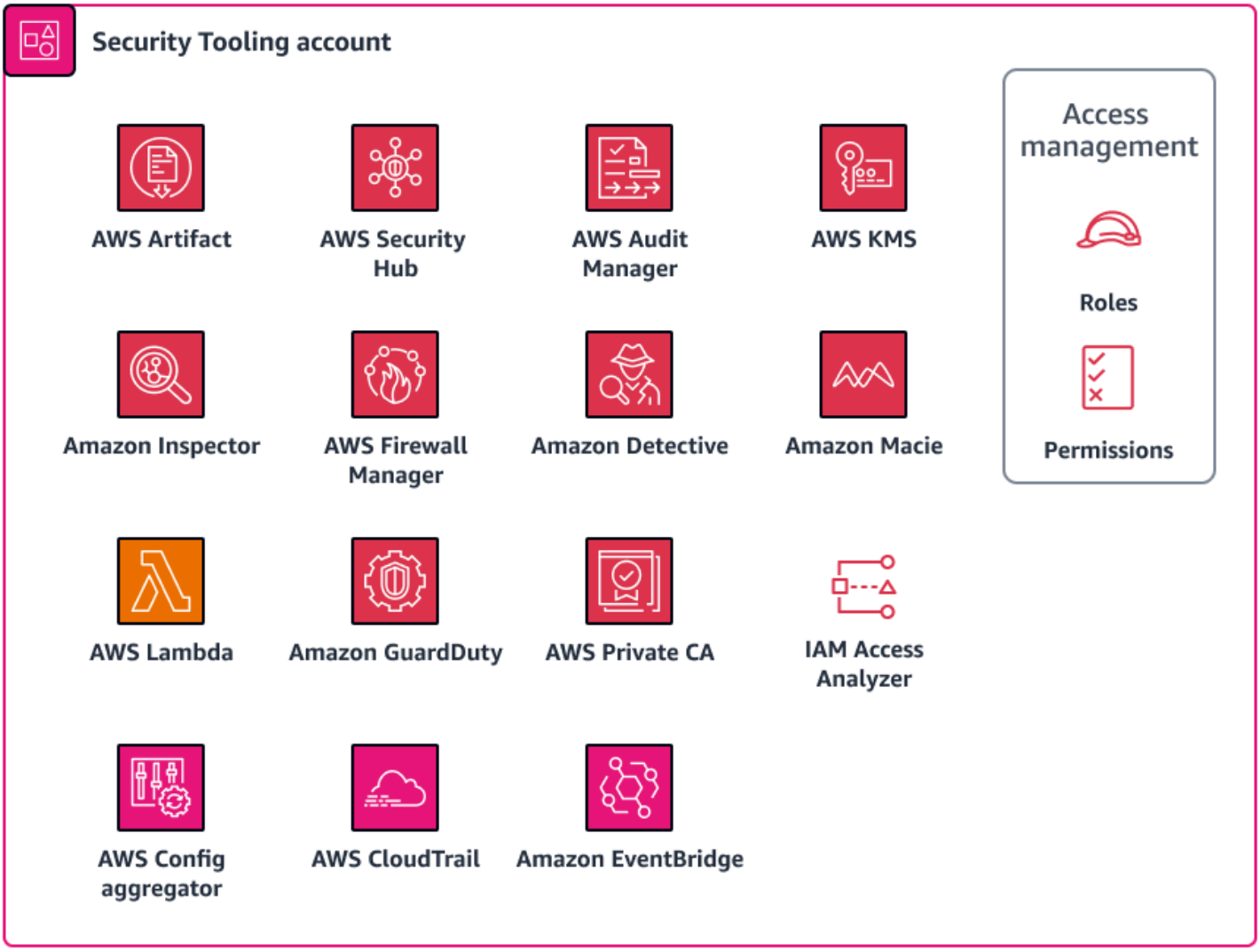
Cuando utilices las etiquetas como un componente fundamental de tu estrategia de control de la privacidad, ten en cuenta lo siguiente:

- Tenga en cuenta las implicaciones de colocar datos personales u otros tipos de datos confidenciales dentro de las claves o valores de las etiquetas. Cuando AWS solicite asistencia técnica, AWS puede analizar las etiquetas y otros identificadores de recursos para ayudar a resolver el problema. En este caso, es posible que desee desidentificar los valores de las etiquetas y, a continuación, volver a identificarlos mediante un sistema controlado por el cliente, como un sistema de gestión de servicios de TI (ITSM). AWS recomienda no incluir información de identificación personal en las etiquetas.
- Tenga en cuenta que algunos valores de las etiquetas deben ser inmutables (no modificables) para evitar que se eludan los controles técnicos, como las condiciones ABAC que se basan en las etiquetas.

Security OU: cuenta de herramientas de seguridad

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

La cuenta Security Tooling está dedicada a operar los servicios fundamentales de seguridad y privacidad, a monitorear Cuentas de AWS y automatizar las alertas y respuestas de seguridad y privacidad. Para obtener más información sobre esta cuenta, consulte la Arquitectura de referencia de AWS seguridad (SRA).AWS El siguiente diagrama ilustra los servicios AWS de seguridad y privacidad que están configurados en la cuenta Security Tooling.



En esta sección se proporciona información más detallada sobre lo siguiente en esta cuenta:

- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- Analizador de acceso de IAM
- Amazon Macie

AWS CloudTrail

AWS CloudTraille ayuda a auditar la actividad general de la API en su Cuenta de AWS. Permitir Regiones de AWS que todos Cuentas de AWS los dispositivos CloudTrail almacenen, procesen o transmitan datos personales puede ayudarlo a rastrear el uso y la divulgación de estos datos. La arquitectura AWS de referencia de seguridad recomienda habilitar un registro de la organización, que es un registro único que registra todos los eventos de todas las cuentas de la organización. Sin embargo, al habilitar este registro organizativo, se agregan los datos de registro multirregionales en un único depósito de Amazon Simple Storage Service (Amazon S3) en la cuenta de Log Archive. En el caso de las cuentas que gestionan datos personales, esto puede implicar algunas consideraciones de diseño adicionales. Los registros pueden contener algunas referencias a datos personales. Para cumplir con sus requisitos de residencia y transferencia de datos, es posible que deba reconsiderar la posibilidad de agregar los datos de registro entre regiones en una sola región donde se encuentra el depósito de S3. Su organización podría considerar qué cargas de trabajo regionales deberían incluirse o excluirse del registro de la organización. Para las cargas de trabajo que decidas excluir del registro de la organización, podrías considerar configurar un registro específico para cada región que oculte los datos personales. Para obtener más información sobre el enmascaramiento de datos personales, consulta la Amazon Data Firehose sección de esta guía. En última instancia, su organización puede tener una combinación de registros organizativos y regionales que se agregan a la cuenta centralizada de Log Archive.

Para obtener más información sobre la configuración de un registro de una sola región, consulta las instrucciones para usar el AWS Command Line Interface (AWS CLI) o la consola. Al crear el registro de la organización, puedes usar una configuración opcional o puedes crear el registro directamente en la CloudTrail consola. AWS Control Tower

Para obtener más información sobre el enfoque general y sobre cómo gestionar la centralización de los registros y los requisitos de transferencia de datos, consulta la Almacenamiento de registros centralizado sección de esta guía. Sea cual sea la configuración que elija, es posible que desee separar la administración de registros en la cuenta de Security Tooling del almacenamiento de

registros en la cuenta de Log Archive, según la AWS SRA. Este diseño le ayuda a crear políticas de acceso con privilegios mínimos para quienes necesitan administrar los registros y quienes necesitan usar los datos de registro.

AWS Config

AWS Configproporciona una vista detallada de sus recursos Cuenta de AWS y de cómo están configurados. Le ayuda a identificar cómo se relacionan los recursos entre sí y cómo han cambiado sus configuraciones a lo largo del tiempo. Para obtener más información sobre cómo se utiliza este servicio en un contexto de seguridad, consulte la Arquitectura AWS de referencia de seguridad.

En AWS Config, puede implementar paquetes de conformidad, que son conjuntos de AWS Config reglas y acciones correctivas. Los paquetes de conformidad proporcionan un marco de uso general diseñado para permitir las comprobaciones de la privacidad, la seguridad, las operaciones y la gobernanza de la optimización de los costes mediante el uso de reglas gestionadas o personalizadas. AWS Config Puede utilizar esta herramienta como parte de un conjunto más amplio de herramientas de automatización para comprobar si las configuraciones de sus AWS recursos cumplen con los requisitos de su propio marco de control.

El paquete de conformidad con las prácticas recomendadas operativas para la versión 1.0 del Marco de privacidad del NIST se ajusta a una serie de controles relacionados con la privacidad del Marco de privacidad del NIST. Cada AWS Config regla se aplica a un tipo de AWS recurso específico y se refiere a uno o más controles del Marco de Privacidad del NIST. Puede usar este paquete de conformidad para realizar un seguimiento del cumplimiento continuo relacionado con la privacidad en todos los recursos de sus cuentas. Las siguientes son algunas de las reglas incluidas en este paquete de conformidad:

- `no-unrestricted-route-to-igw`— Esta regla ayuda a evitar la exfiltración de datos en el plano de datos mediante la supervisión continua de las tablas de enrutamiento de VPC en busca de rutas `0.0.0.0/0` predeterminadas `::/0` o de salida a una puerta de enlace de Internet. Esto le ayuda a restringir dónde se puede enviar el tráfico con destino a Internet, especialmente si hay rangos de CIDR que se sabe que son maliciosos.
- `encrypted-volumes`— Esta regla comprueba si los volúmenes de Amazon Elastic Block Store (Amazon EBS) adjuntos a las instancias de Amazon Elastic Compute Cloud (EC2Amazon) están cifrados. Si su organización tiene requisitos de control específicos relacionados con el uso de claves AWS Key Management Service (AWS KMS) para proteger los datos personales, puede especificar una clave específica IDs como parte de la regla para comprobar que los volúmenes estén cifrados con una clave específica AWS KMS .

- `restricted-common-ports`— Esta regla comprueba si los grupos de EC2 seguridad de Amazon permiten el tráfico TCP sin restricciones a puertos específicos. Los grupos de seguridad pueden ayudarlo a administrar el acceso a la red al proporcionar un filtrado detallado del tráfico de red de entrada y salida a los recursos. AWS Bloquear el tráfico de entrada de sus recursos `0.0.0.0/0` a puertos comunes, como el TCP 3389 y el TCP 21, le ayuda a restringir el acceso remoto.

AWS Config se puede utilizar para realizar comprobaciones de conformidad proactivas y reactivas de sus AWS recursos. Además de tener en cuenta las reglas que se encuentran en los paquetes de conformidad, puede incorporarlas en los modos de evaluación preventiva y proactiva. Esto ayuda a implementar las comprobaciones de privacidad en una fase más temprana del ciclo de vida del desarrollo del software, ya que los desarrolladores de aplicaciones pueden empezar a incorporar las comprobaciones previas a la implementación. Por ejemplo, pueden incluir enlaces en sus AWS CloudFormation plantillas que comprueben el recurso declarado en la plantilla con respecto a todas las AWS Config reglas relacionadas con la privacidad que tienen habilitado el modo proactivo. Para obtener más información, consulte AWS Config Rules Now Support Proactive Compliance (entrada del AWS blog).

Amazon GuardDuty

AWS ofrece varios servicios que pueden usarse para almacenar o procesar datos personales, como Amazon S3, Amazon Relational Database Service (Amazon RDS) o EC2 Amazon with Kubernetes. Amazon GuardDuty combina la visibilidad inteligente con la supervisión continua para detectar indicadores que puedan estar relacionados con la divulgación no intencionada de datos personales. Para obtener más información sobre cómo se utiliza este servicio en un contexto de seguridad, consulte la arquitectura de referencia AWS de seguridad.

Con él GuardDuty, puede identificar actividades potencialmente maliciosas relacionadas con la privacidad a lo largo del ciclo de vida de un ataque. Por ejemplo, GuardDuty puede avisarte sobre conexiones a sitios incluidos en listas negras, tráfico o volúmenes de tráfico inusuales en los puertos de red, filtraciones de DNS, lanzamientos inesperados de EC2 instancias o llamadas inusuales por parte de un ISP. También puede configurarlo GuardDuty para detener las alertas de direcciones IP confiables de sus propias listas de IP confiables y alertar sobre direcciones IP malintencionadas conocidas de sus propias listas de amenazas.

Como se recomienda en la AWS SRA, puede habilitar la cuenta Security Tooling GuardDuty para todos los Cuentas de AWS miembros de su organización y configurarla como administrador GuardDuty delegado. GuardDutyagrupa los hallazgos de toda la organización en esta cuenta única.

Para obtener más información, consulte Administrar GuardDuty cuentas con AWS Organizations. También puedes considerar la posibilidad de identificar a todas las partes interesadas relacionadas con la privacidad en el proceso de respuesta a los incidentes, desde la detección y el análisis hasta la contención y la erradicación, e implicarlas en cualquier incidente que pueda implicar la exfiltración de datos.

Analizador de acceso de IAM

Muchos clientes quieren tener la seguridad permanente de que los datos personales se comparten de forma adecuada con los procesadores externos previamente aprobados y previstos, y no con otras entidades. Un perímetro de datos es un conjunto de barreras preventivas diseñadas para permitir que solo las identidades confiables de las redes esperadas accedan a los recursos confiables de su entorno. AWS Al definir los controles para la divulgación intencionada o no intencionada de datos personales, puede definir las identidades confiables, los recursos confiables y las redes esperadas.

Con AWS Identity and Access Management Access Analyzer (IAM Access Analyzer), las organizaciones pueden definir una Cuenta de AWS zona de confianza y configurar alertas en caso de infracciones en esa zona de confianza. IAM Access Analyzer analiza las políticas de IAM para ayudar a identificar y resolver el acceso no intencionado público o entre cuentas a recursos potencialmente confidenciales. IAM Access Analyzer utiliza la lógica matemática y la inferencia para generar conclusiones exhaustivas sobre los recursos a los que se puede acceder desde fuera de un. Cuenta de AWS Por último, para responder a las políticas de IAM excesivamente permisivas y corregirlas, puede utilizar IAM Access Analyzer para validar las políticas existentes comparándolas con las mejores prácticas de IAM y ofrecer sugerencias. IAM Access Analyzer puede generar una política de IAM con privilegios mínimos que se base en la actividad de acceso previa de un director de IAM. Analiza CloudTrail los registros y genera una política que concede únicamente los permisos necesarios para seguir realizando esas tareas.

Para obtener más información sobre cómo se utiliza IAM Access Analyzer en un contexto de seguridad, consulte la Arquitectura de referencia AWS de seguridad.

Amazon Macie

Amazon Macie es un servicio que utiliza el aprendizaje automático y la coincidencia de patrones para descubrir datos confidenciales, proporciona visibilidad de los riesgos de seguridad de los datos y le ayuda a automatizar las protecciones contra esos riesgos. Macie genera resultados cuando detecta posibles infracciones de las políticas o problemas con la seguridad o la privacidad de sus buckets de Amazon S3. Macie es otra herramienta que las organizaciones pueden utilizar

para implementar la automatización con el fin de respaldar los esfuerzos de cumplimiento. Para obtener más información sobre cómo se utiliza este servicio en un contexto de seguridad, consulte la Arquitectura de referencia AWS de seguridad.

Macie puede detectar una lista amplia y creciente de tipos de datos confidenciales, incluida la información de identificación personal (PII), como nombres, direcciones y otros atributos identificables. Incluso puede crear identificadores de datos personalizados para definir los criterios de detección que reflejen la definición de datos personales de su organización.

A medida que su organización defina controles preventivos para sus depósitos de Amazon S3 que contienen datos personales, puede utilizar Macie como mecanismo de validación para garantizar continuamente dónde se encuentran sus datos personales y cómo están protegidos. Para empezar, habilite Macie y configure la detección automática de datos confidenciales. Macie analiza continuamente los objetos de todos sus depósitos de S3, en todas las cuentas y. Regiones de AWS Macie genera y mantiene un mapa térmico interactivo que muestra dónde se encuentran los datos personales. La función de descubrimiento automatizado de datos confidenciales está diseñada para reducir los costos y minimizar la necesidad de configurar manualmente las tareas de descubrimiento. Puede aprovechar la función de descubrimiento automatizado de datos confidenciales y utilizar Macie para detectar automáticamente nuevos depósitos o nuevos datos en los depósitos existentes y, a continuación, validarlos con las etiquetas de clasificación de datos asignadas. Configure esta arquitectura para notificar oportunamente a los equipos de desarrollo y privacidad correspondientes sobre los depósitos mal clasificados o no clasificados.

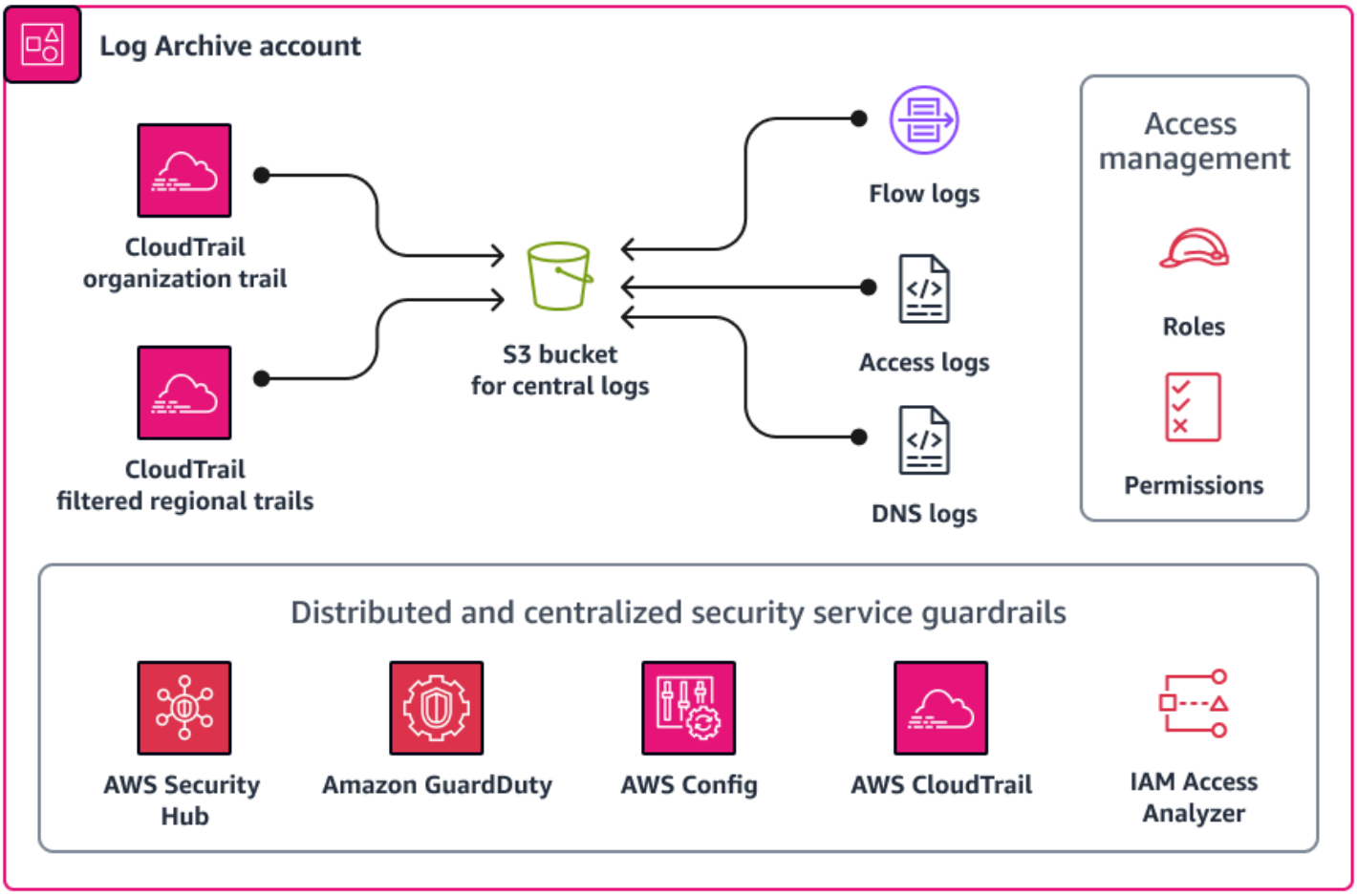
Puede habilitar Macie para todas las cuentas de su organización mediante. AWS Organizations Para obtener más información, consulte Integración y configuración de una organización en Amazon Macie.

Cuenta Security OU — Log Archive

> Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

La cuenta de Log Archive es el lugar donde se centralizan los tipos de registros de infraestructura, servicios y aplicaciones. Para obtener más información sobre esta cuenta, consulte la Arquitectura AWS de referencia de seguridad (AWS SRA). Con una cuenta dedicada a los registros, puede aplicar alertas coherentes en todos los tipos de registros y confirmar que el personal de respuesta a incidentes puede acceder a un conjunto de estos registros desde un solo lugar. También puedes

configurar los controles de seguridad y las políticas de retención de datos desde un solo lugar, lo que puede simplificar la sobrecarga operativa en materia de privacidad. El siguiente diagrama ilustra los servicios AWS de seguridad y privacidad que están configurados en la cuenta de Log Archive.



Almacenamiento de registros centralizado

Los archivos de registro (como AWS CloudTrail los registros) pueden contener información que podría considerarse datos personales. Algunas organizaciones optan por utilizar un registro organizativo para agrupar CloudTrail los registros de todas Regiones de AWS las cuentas en una ubicación central, por motivos de visibilidad. Para obtener más información, consulte la sección AWS CloudTrail de esta guía. Al implementar la centralización de CloudTrail los registros, estos se almacenan normalmente en un bucket de Amazon Simple Storage Service (Amazon S3) en una sola región.

En función de la definición de datos personales de su organización y de las normas de privacidad regionales aplicables, es posible que deba plantearse la posibilidad de realizar transferencias de

datos transfronterizas. Si su organización necesita cumplir con los requisitos de transferencia de datos de las normas de privacidad regionales, las siguientes opciones pueden ayudarle:

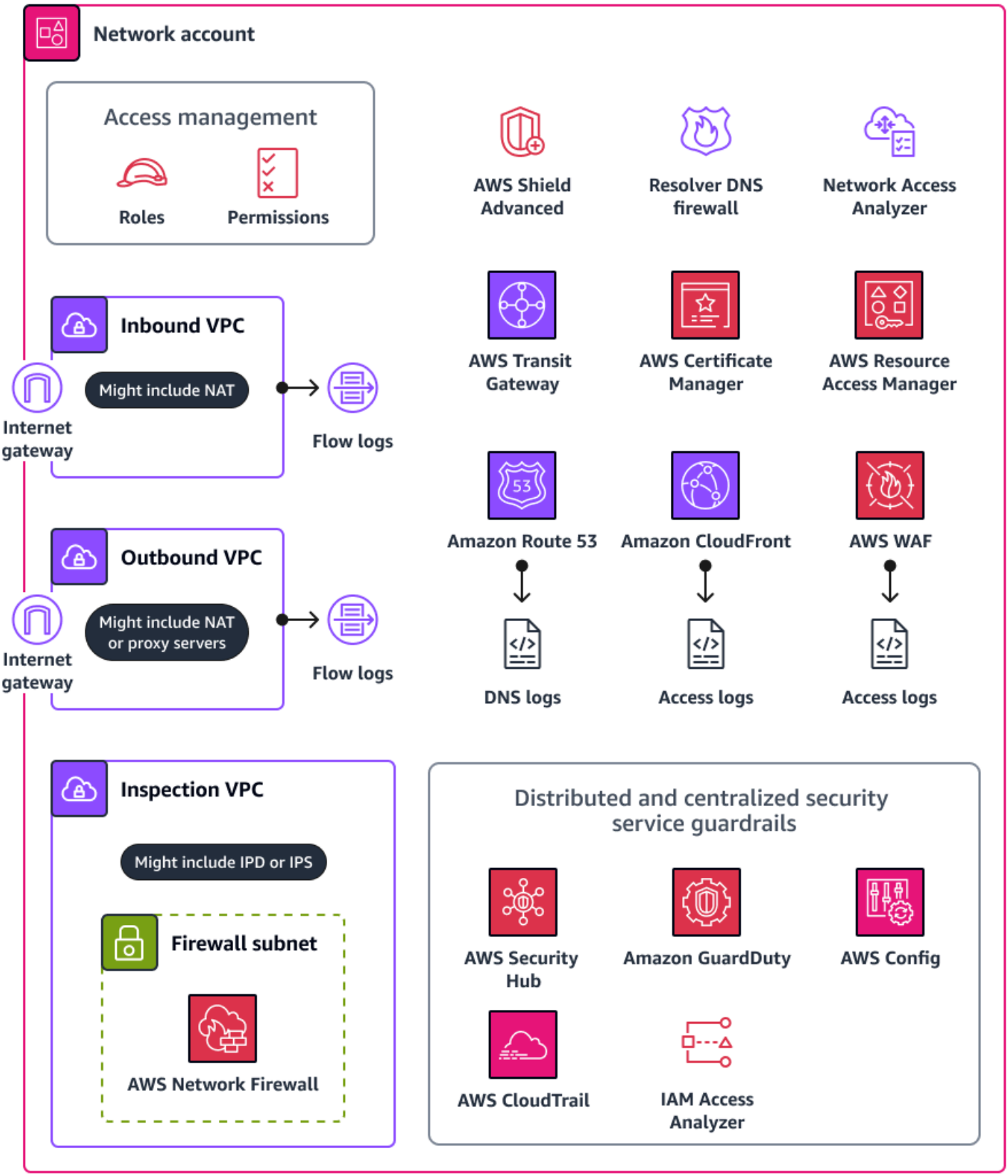
1. Si su organización presta servicios Nube de AWS a interesados de varios países, puede optar por agregar todos los registros del país que tenga los requisitos de residencia de datos más estrictos. Por ejemplo, si opera en Alemania y tiene los requisitos más estrictos, puede agregar datos en un depósito de S3 para que `eu-central-1` Región de AWS los datos recopilados en Alemania no salgan de las fronteras de Alemania. Para esta opción, puede configurar un registro organizativo único CloudTrail que agregue los registros de todas las cuentas y de Regiones de AWS la región de destino.
2. Redacte los datos personales que deben permanecer en ella Región de AWS antes de copiarlos y agregarlos a otra región. Por ejemplo, puede ocultar los datos personales de la región anfitriona de la aplicación antes de transferir los registros a otra región. Para obtener más información sobre el enmascaramiento de datos personales, consulte la Amazon Data Firehose sección de esta guía.

Trabaje con su asesor legal para determinar qué datos personales están incluidos en el ámbito de aplicación y qué AWS Region-to-Region transferencias están permitidas.

Unidad organizativa de infraestructura: cuenta de red

> Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

En la cuenta de red, usted administra las redes entre sus nubes privadas virtuales (VPCs) e Internet en general. En esta cuenta, puedes implementar amplios mecanismos de control de la divulgación mediante AWS WAF, use AWS Resource Access Manager (AWS RAM) para compartir subredes y AWS Transit Gateway archivos adjuntos de VPC, y usar Amazon CloudFront para respaldar el uso específico de los servicios. Para obtener más información sobre esta cuenta, consulte la Arquitectura de referencia AWS de seguridad (AWS SRA). El siguiente diagrama ilustra los servicios AWS de seguridad y privacidad que están configurados en la cuenta de red.


Network account
Access management
Roles
Permissions
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Transit Gateway
AWS Certificate Manager
AWS Resource Access Manager
Amazon Route 53
Amazon CloudFront
AWS WAF
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
DNS logs
Access logs
Access logs
Inspection VPC
Might include IPD or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

En esta sección se proporciona información más detallada sobre lo siguiente Servicios de AWS que se utiliza en esta cuenta:

- Amazon CloudFront
- AWS Resource Access Manager
- AWS Transit Gateway
- AWS WAF

Amazon CloudFront

Amazon CloudFront admite restricciones geográficas para las aplicaciones frontend y el alojamiento de archivos. CloudFrontpuede entregar contenido a través de una red mundial de centros de datos que se denominan ubicaciones periféricas. Cuando un usuario solicita el contenido con el que estás publicando CloudFront, la solicitud se redirige a la ubicación perimetral que ofrezca la latencia más baja. Para obtener más información sobre cómo se utiliza este servicio en un contexto de seguridad, consulte la Arquitectura de referencia AWS de seguridad.

Puede utilizar restricciones CloudFront geográficas para impedir que los usuarios de ubicaciones geográficas específicas accedan al contenido que está distribuyendo a través de una CloudFront distribución. Para obtener más información y opciones de configuración para las restricciones geográficas, consulte Restringir la distribución geográfica del contenido en la CloudFront documentación.

También puede configurarlo CloudFront para generar registros de acceso que contengan información detallada sobre cada solicitud de usuario que CloudFront reciba. Para obtener más información, consulte Configuración y uso de registros estándar (registros de acceso) en la CloudFront documentación. Por último, si CloudFront está configurado para almacenar en caché el contenido en una serie de ubicaciones de borde, podría considerar dónde se produce el almacenamiento en caché. Para algunas organizaciones, el almacenamiento en caché transregional puede estar sujeto a requisitos de transferencia de datos transfronteriza.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) le ayuda a compartir sus recursos de forma segura Cuentas de AWS para reducir la sobrecarga operativa y proporcionar visibilidad y auditabilidad. De AWS RAM este modo, las organizaciones pueden restringir qué AWS recursos se pueden compartir con otras personas Cuentas de AWS de su organización o con cuentas de terceros. Para obtener

más información, consulta AWS Recursos que se pueden compartir. En la cuenta de red, puede utilizarla AWS RAM para compartir subredes de VPC y conexiones de puerta de enlace de tránsito. Si solías AWS RAM compartir una conexión de plano de datos con otra Cuenta de AWS, considera la posibilidad de establecer procesos para comprobar que las conexiones se realizan según las aprobaciones previas. Regiones de AWS

Además de compartir VPCs y transitar las conexiones de pasarela, se AWS RAM puede utilizar para compartir recursos que no son compatibles con las políticas de IAM basadas en recursos. En el caso de una carga de trabajo alojada en la unidad organizativa de datos personales, puede utilizarla AWS RAM para acceder a los datos personales que se encuentran en una unidad organizativa independiente. Cuenta de AWS Para obtener más información, consulte AWS Resource Access Manager la sección sobre la cuenta de la aplicación OU — PD de datos personales.

AWS Transit Gateway

Si desea implementar AWS recursos que recopilen, almacenen o procesen datos personales de manera Regiones de AWS que se ajusten a los requisitos de residencia de los datos de su organización y cuenta con las garantías técnicas adecuadas, considere la posibilidad de implementar barreras de protección para evitar flujos de datos transfronterizos no aprobados en los planos de control y datos. En el plano de control, puede limitar el uso regional y, en consecuencia, los flujos de datos entre regiones mediante políticas de control de servicios y de IAM.

Existen varias opciones para controlar los flujos de datos entre regiones en el plano de datos. Por ejemplo, puede usar tablas de enrutamiento, interconexión de VPC y adjuntos. AWS Transit Gateway AWS Transit Gatewayes un centro central que conecta nubes privadas virtuales (VPCs) y redes locales. Como parte de su mayor zona de aterrizaje de AWS, puede considerar las diversas formas en que pueden circular los datos, por ejemplo Regiones de AWS, a través de las puertas de enlace de Internet, a través de la interconexión directa y a través VPC-to-VPC de la interconexión interregional. AWS Transit Gateway Por ejemplo, puede hacer lo siguiente en: AWS Transit Gateway

- Confirme que las conexiones este-oeste y norte-sur entre sus entornos VPCs y los locales cumplen con sus requisitos de privacidad.
- Configure los ajustes de la VPC de acuerdo con sus requisitos de privacidad.
- Utilice una política de control de servicios en AWS Organizations las políticas de IAM para evitar modificaciones en su configuración AWS Transit Gateway y en la de Amazon Virtual Private Cloud (Amazon VPC). Para ver un ejemplo de política de control de servicios, consulte esta Restringir los cambios en las configuraciones de VPC guía.

AWS WAF

Para evitar la divulgación no intencionada de datos personales, puede implementar un defense-in-depth enfoque para sus aplicaciones web. Puede incorporar la validación de entrada y la limitación de velocidad en su aplicación, pero AWS WAF puede servir como otra línea de defensa. AWS WAFes un firewall de aplicaciones web que le ayuda a supervisar las solicitudes HTTP y HTTPS que se reenvían a los recursos de sus aplicaciones web protegidas. Para obtener más información sobre cómo se utiliza este servicio en un contexto de seguridad, consulte la Arquitectura AWS de referencia de seguridad.

Con AWS WAF ella, puede definir e implementar reglas que inspeccionen en función de criterios específicos. Las siguientes actividades pueden estar asociadas a la divulgación no intencionada de datos personales:

- Tráfico procedente de direcciones IP o ubicaciones geográficas desconocidas o maliciosas
- Los 10 principales ataques del Open Worldwide Application Security Project (OWASP), incluidos los relacionados con la exfiltración, como la inyección de SQL
- Altas tasas de solicitudes
- Tráfico general de bots
- Raspadores de contenido

Puede implementar grupos de AWS WAF reglas gestionados por. AWS Algunos grupos de reglas gestionados se AWS WAF pueden utilizar para detectar amenazas a la privacidad y los datos personales, por ejemplo:

- Base de datos SQL: este grupo de reglas contiene reglas diseñadas para bloquear los patrones de solicitud asociados con la explotación de las bases de datos SQL, como los ataques de inyección de SQL. Tenga en cuenta este grupo de reglas si su aplicación interactúa con una base de datos SQL.
- Entradas incorrectas conocidas: este grupo de reglas contiene reglas diseñadas para bloquear los patrones de solicitud que se sabe que no son válidos y que están asociados con la explotación o el descubrimiento de vulnerabilidades.
- Control de bots: este grupo de reglas contiene reglas diseñadas para gestionar las solicitudes de los bots, que pueden consumir un exceso de recursos, distorsionar las métricas empresariales, provocar tiempos de inactividad y realizar actividades maliciosas.

- Prevención de apropiación de cuentas (ATP): este grupo de reglas contiene reglas diseñadas para evitar intentos malintencionados de apropiación de cuentas. Este grupo de reglas inspecciona los intentos de inicio de sesión enviados al punto final de inicio de sesión de la aplicación.

Datos personales: OU: cuenta de aplicación PDF

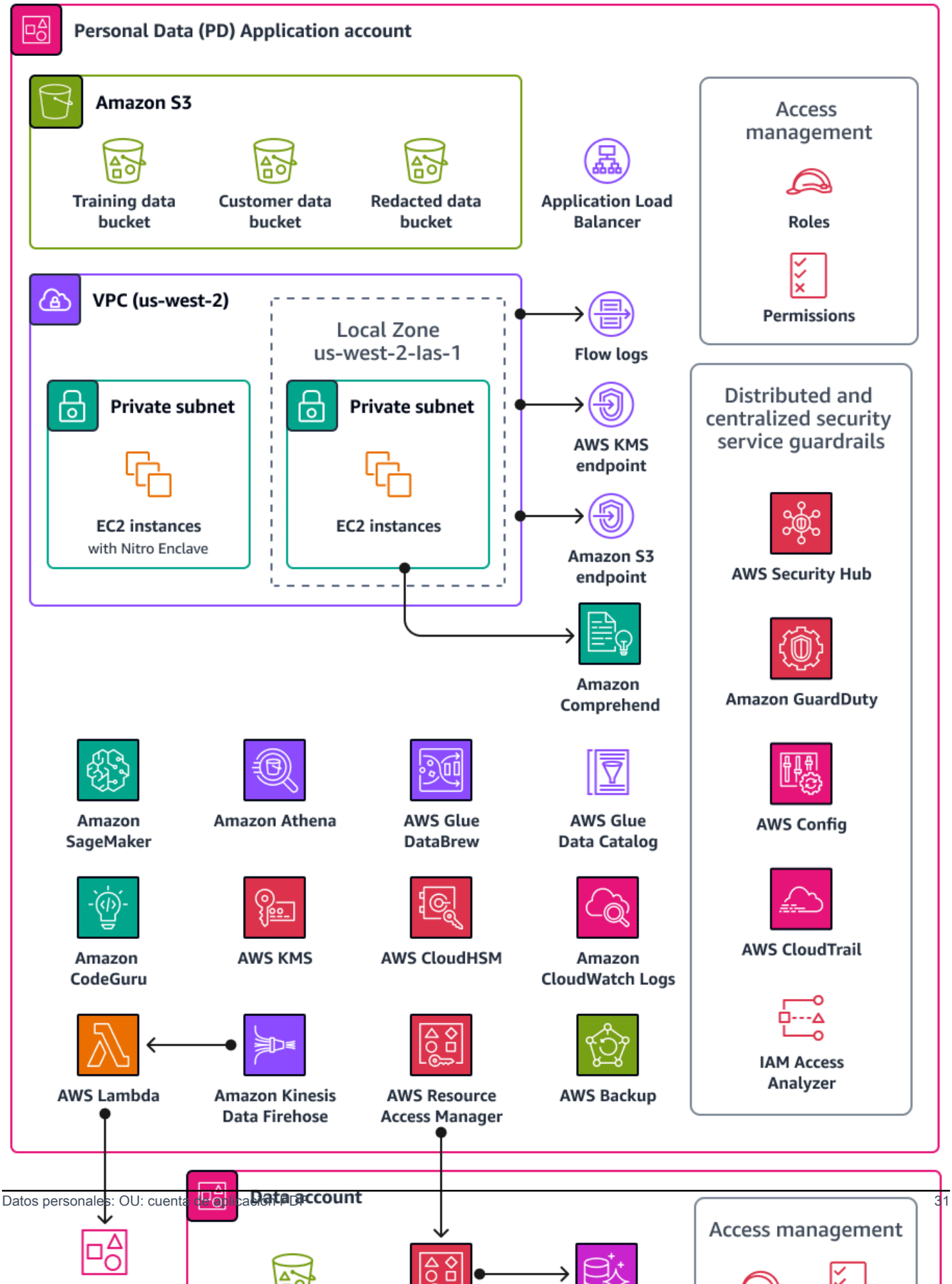
Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

La cuenta de la solicitud de datos personales (PD) es el lugar donde su organización aloja los servicios que recopilan y procesan datos personales. En concreto, puede almacenar lo que define como datos personales en esta cuenta. La AWS PRA muestra varios ejemplos de configuraciones de privacidad a través de una arquitectura web sin servidor de varios niveles. Cuando se trata de operar cargas de trabajo en una AWS landing zone, las configuraciones de privacidad no deben considerarse one-size-fits-all soluciones. Por ejemplo, su objetivo podría ser comprender los conceptos subyacentes, cómo pueden mejorar la privacidad y cómo su organización puede aplicar las soluciones a sus arquitecturas y casos de uso particulares.

Cuentas de AWS En su organización que recopila, almacena o procesa datos personales, puede utilizar AWS Organizations e AWS Control Tower implementar barreras fundamentales y repetibles. Es fundamental establecer una unidad organizativa (OU) dedicada a estas cuentas. Por ejemplo, es posible que desee aplicar barreras de residencia de datos solo a un subconjunto de cuentas en las que la residencia de los datos sea una consideración de diseño fundamental. Para muchas organizaciones, estas son las cuentas que almacenan y procesan los datos personales.

Su organización puede admitir una cuenta de datos dedicada, que es donde almacena la fuente autorizada de sus conjuntos de datos personales. Una fuente de datos autorizada es una ubicación en la que se almacena la versión principal de los datos, que podría considerarse la versión más fiable y precisa de los datos. Por ejemplo, puede copiar los datos de la fuente de datos autorizada a otras ubicaciones, como los depósitos de Amazon Simple Storage Service (Amazon S3) en la cuenta de la aplicación PD que se utilizan para almacenar datos de entrenamiento, un subconjunto de datos de clientes y datos redactados. Al adoptar este enfoque multicuenta para separar los conjuntos de datos personales completos y definitivos de la cuenta de datos de las cargas de trabajo de los consumidores intermedios de la cuenta de la aplicación PD, puede reducir el alcance del impacto en caso de acceso no autorizado a sus cuentas.

El siguiente diagrama ilustra los servicios de AWS seguridad y privacidad que están configurados en las cuentas de datos y aplicaciones de PD.


Personal Data (PD) Application account
Amazon S3
Training data bucket
Customer data bucket
Redacted data bucket
Application Load Balancer
Access management
Roles
Permissions
VPC (us-west-2)
Local Zone us-west-2-las-1
Private subnet
EC2 instances with Nitro Enclave
Private subnet
EC2 instances
Flow logs
AWS KMS endpoint
Amazon S3 endpoint
Amazon Comprehend
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon SageMaker
Amazon Athena
AWS Glue DataBrew
AWS Glue Data Catalog
Amazon CodeGuru
AWS KMS
AWS CloudHSM
Amazon CloudWatch Logs
AWS Lambda
Amazon Kinesis Data Firehose
AWS Resource Access Manager
AWS Backup
Log Archive
Data account
Access management

En esta sección se proporciona información más detallada sobre lo siguiente Servicios de AWS que se utiliza en estas cuentas:

- Amazon Athena
- Amazon CloudWatch Logs
- CodeGuru Revisor de Amazon
- Amazon Comprehend
- Amazon Data Firehose
- AWS Glue
- AWS Key Management Service
- AWS Zonas Locales
- AWS Nitro Enclaves
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker AI
- AWS funciones que ayudan a gestionar el ciclo de vida de los datos
- Servicios y características de AWS que ayudan a segmentar los datos

Amazon Athena

También puedes considerar los controles de limitación de las consultas de datos para cumplir tus objetivos de privacidad. Amazon Athena es un servicio de consultas interactivo que facilita el análisis de datos en Amazon S3 con SQL estándar. No es necesario cargar los datos en Athena; funciona directamente con los datos almacenados en los cubos S3.

Un caso de uso común de Athena es proporcionar a los equipos de análisis de datos conjuntos de datos personalizados y saneados. Si los conjuntos de datos contienen datos personales, puede desinfectarlos ocultando columnas enteras de datos personales que proporcionan poco valor a los equipos de análisis de datos. Para obtener más información, consulte Anonimizar y administrar los datos de su lago de datos con Amazon Athena y AWS Lake Formation (entrada del blog).AWS

Si su enfoque de transformación de datos requiere flexibilidad adicional fuera de las funciones compatibles con Athena, puede definir funciones personalizadas, denominadas funciones definidas por el usuario (UDF). Puede invocar UDFs una consulta SQL enviada a Athena y se ejecutará.

AWS Lambda Puede utilizar `FILTER SQL` consultas UDFs de entrada `SELECT` y, además, puede invocar varias UDFs en la misma consulta. Por motivos de privacidad, puede crear UDFs dispositivos que utilicen tipos específicos de enmascaramiento de datos, como mostrar solo los últimos cuatro caracteres de cada valor de una columna.

Amazon CloudWatch Logs

Amazon CloudWatch Logs le ayuda a centralizar los registros de todos sus sistemas y aplicaciones Servicios de AWS para que pueda supervisarlos y archivarlos de forma segura. En CloudWatch Logs, puede utilizar una política de protección de datos para los grupos de registros nuevos o existentes a fin de minimizar el riesgo de divulgación de datos personales. Las políticas de protección de datos pueden detectar datos confidenciales, como datos personales, en sus registros. La política de protección de datos puede enmascarar esos datos cuando los usuarios acceden a los registros a través del AWS Management Console. Cuando los usuarios necesiten acceder directamente a los datos personales, de acuerdo con la especificación de propósito general de su carga de trabajo, puede asignar `logs:Unmask` permisos a esos usuarios. También puede crear una política de protección de datos para toda la cuenta y aplicarla de forma coherente en todas las cuentas de su organización. Esto configura el enmascaramiento de forma predeterminada para todos los grupos de registros actuales y futuros en CloudWatch Logs. También le recomendamos que habilite los informes de auditoría y los envíe a otro grupo de registros, a un bucket de Amazon S3 o a Amazon Data Firehose. Estos informes contienen un registro detallado de los resultados de protección de datos en cada grupo de registros.

CodeGuru Revisor de Amazon

Tanto para la privacidad como para la seguridad, es vital para muchas organizaciones que respalden el cumplimiento continuo durante las fases de implementación y posteriores a la implementación. La AWS PRA incluye controles proactivos en los procesos de implementación de las aplicaciones que procesan datos personales. Amazon CodeGuru Reviewer puede detectar posibles defectos que podrían exponer datos personales en código Java y Python. JavaScript Ofrece sugerencias a los desarrolladores para mejorar el código. CodeGuru El revisor puede identificar los defectos en una amplia gama de prácticas recomendadas generales, de seguridad y de privacidad. Para obtener más información, consulta la biblioteca de Amazon CodeGuru Detector. Está diseñado para funcionar con varios proveedores de fuentes AWS CodeCommit, incluidos Bitbucket y Amazon S3. GitHub Algunos de los defectos relacionados con la privacidad que CodeGuru Reviewer puede detectar incluyen:

- Inyección de SQL
- Cookies no seguras

- Falta la autorización
- Recrificación del lado del cliente AWS KMS

Amazon Comprehend

Amazon Comprehend es un servicio de procesamiento del lenguaje natural (PNL) que utiliza el aprendizaje automático para descubrir información y conexiones valiosas en documentos de texto en inglés. Amazon Comprehend puede detectar y redactar datos personales en documentos de texto estructurados, semiestructurados o no estructurados. Para obtener más información, consulte Información de identificación personal (PII) en la documentación de Amazon Comprehend.

Puede utilizar la API de AWS SDKs y Amazon Comprehend para integrar Amazon Comprehend con muchas aplicaciones. Un ejemplo es el uso de Amazon Comprehend para detectar y redactar datos personales con Amazon S3 Object Lambda. Las organizaciones pueden usar S3 Object Lambda para añadir código personalizado a las solicitudes GET de Amazon S3 para modificar y procesar los datos a medida que se devuelven a una aplicación. S3 Object Lambda puede filtrar filas, cambiar el tamaño de las imágenes de forma dinámica, redactar datos personales y mucho más. Gracias a AWS Lambda sus funciones, el código se ejecuta en una infraestructura totalmente gestionada AWS, lo que elimina la necesidad de crear y almacenar copias derivadas de los datos o de ejecutar proxies. No necesita cambiar sus aplicaciones para transformar objetos con S3 Object Lambda. Puede utilizar la función `ComprehendPiiRedactionS3Object` Lambda AWS Serverless Application Repository para redactar datos personales. Esta función utiliza Amazon Comprehend para detectar entidades de datos personales y las redacta sustituyéndolas por asteriscos. Para obtener más información, consulte Detección y redacción de datos de PII con S3 Object Lambda y Amazon Comprehend en la documentación de Amazon S3.

Como Amazon Comprehend tiene muchas opciones para la integración de aplicaciones a través de AWS SDKs, puede usar Amazon Comprehend para identificar datos personales en muchos lugares diferentes donde recopila, almacena y procesa datos. Puede utilizar las capacidades de Amazon Comprehend ML para detectar y redactar datos personales en los registros de aplicaciones (entrada de AWS blog), los correos electrónicos de los clientes, los tickets de soporte y mucho más. El diagrama de arquitectura de la cuenta PD Application muestra cómo puedes realizar esta función para los registros de aplicaciones en Amazon EC2. Amazon Comprehend ofrece dos modos de redacción:

- `REPLACE_WITH_PII_ENTITY_TYPE`reemplaza cada entidad de PII por sus tipos. Por ejemplo, Jane Doe se sustituiría por NAME.

- `MASK`reemplaza los caracteres de las entidades PII por un carácter de su elección (! , #, $,%, &, o @). Por ejemplo, Jane Doe podría sustituirse por **** ***.

Amazon Data Firehose

Amazon Data Firehose se puede utilizar para capturar, transformar y cargar datos de streaming en servicios descendentes, como Amazon Managed Service para Apache Flink o Amazon S3. Firehose se suele utilizar para transportar grandes cantidades de datos de streaming, como registros de aplicaciones, sin tener que construir canalizaciones de procesamiento desde cero.

Puede utilizar las funciones de Lambda para realizar un procesamiento personalizado o integrado antes de que los datos se envíen aguas abajo. En aras de la privacidad, esta capacidad admite los requisitos de minimización de datos y transferencia de datos transfronteriza. Por ejemplo, puede usar Lambda y Firehose para transformar los datos de registro de varias regiones antes de que se centralicen en la cuenta de Log Archive. Para obtener más información, consulte Biogen: solución de registro centralizada para cuentas múltiples (vídeo). YouTube En la cuenta de PD Application, configuras Amazon CloudWatch AWS CloudTrail para enviar los registros a una transmisión de entrega de Firehose. Una función Lambda transforma los registros y los envía a un bucket S3 central de la cuenta de Log Archive. Puede configurar la función Lambda para enmascarar campos específicos que contienen datos personales. Esto ayuda a evitar la transferencia de datos personales de un lado a otro Regiones de AWS. Al utilizar este enfoque, los datos personales se ocultan antes de la transferencia y la centralización, y no después. En el caso de las solicitudes presentadas en jurisdicciones que no están sujetas a los requisitos de transferencia transfronteriza, suele ser más eficiente desde el punto de vista operativo y rentable agregar los registros a lo largo del proceso organizativo. CloudTrail Para obtener más información, consulte la sección AWS CloudTrail de esta guía dedicada a la unidad organizativa sobre seguridad (Security Tooling).

AWS Glue

El mantenimiento de conjuntos de datos que contienen datos personales es un componente clave de Privacy by Design. Los datos de una organización pueden estar estructurados, semiestructurados o no estructurados. Los conjuntos de datos personales sin estructura pueden dificultar la realización de una serie de operaciones que mejoran la privacidad, como la minimización de los datos, el rastreo de los datos atribuidos a un solo sujeto de datos como parte de una solicitud del interesado, la garantía de una calidad de datos uniforme y la segmentación general de los conjuntos de datos. AWS Gluees un servicio de extracción, transformación y carga (ETL) totalmente gestionado. Puede ayudarle a clasificar, limpiar, enriquecer y mover datos entre almacenes de datos y flujos de datos. AWS Glue

las funciones están diseñadas para ayudarlo a descubrir, preparar, estructurar y combinar conjuntos de datos para el análisis, el aprendizaje automático y el desarrollo de aplicaciones. Puede utilizarlas AWS Glue para crear una estructura común y predecible sobre sus conjuntos de datos existentes. AWS Glue Data Catalog AWS Glue DataBrew, y la calidad de AWS Glue los datos son AWS Glue funciones que pueden ayudar a cumplir los requisitos de privacidad de su organización.

AWS Glue Data Catalog

AWS Glue Data Catalogle ayuda a establecer conjuntos de datos fáciles de mantener. El catálogo de datos contiene referencias a los datos que se utilizan como fuentes y destinos para las tareas de extracción, transformación y carga (ETL). AWS Glue La información del catálogo de datos se almacena como tablas de metadatos y cada tabla especifica un único banco de datos. Se ejecuta un AWS Glue rastreador para hacer un inventario de los datos de diversos tipos de almacenes de datos. Agrega clasificadores integrados y personalizados al rastreador, y estos clasificadores deducen el formato y el esquema de los datos personales. A continuación, el rastreador escribe los metadatos en el catálogo de datos. Una tabla de metadatos centralizada puede facilitar la respuesta a las solicitudes de los interesados (como el derecho a la supresión), ya que añade estructura y previsibilidad a las distintas fuentes de datos personales de su entorno. AWS Para ver un ejemplo completo de cómo utilizar Data Catalog para responder automáticamente a estas solicitudes, consulte Gestión de las solicitudes de borrado de datos en su lago de datos con Amazon S3 Find and Forget (entrada del AWS blog). Por último, si su organización utiliza bases de datos, tablas, filas y celdas AWS Lake Formationpara administrar y proporcionar un acceso detallado a ellas, el catálogo de datos es un componente clave. Data Catalog permite compartir datos entre cuentas y le ayuda a utilizar el control de acceso basado en etiquetas para gestionar su lago de datos a escala (entrada del blog).AWS

AWS Glue DataBrew

AWS Glue DataBrewle ayuda a limpiar y normalizar los datos, y puede realizar transformaciones en los datos, como eliminar o enmascarar la información de identificación personal y cifrar los campos de datos confidenciales de las canalizaciones de datos. También puede mapear visualmente el linaje de sus datos para comprender las distintas fuentes de datos y los pasos de transformación por los que han pasado los datos. Esta función adquiere cada vez más importancia a medida que su organización trabaja para comprender y rastrear mejor la procedencia de los datos personales. DataBrew le ayuda a ocultar los datos personales durante la preparación de los datos. Puede detectar datos personales como parte de una labor de elaboración de perfiles de datos y recopilar estadísticas, como el número de columnas que pueden contener datos personales y las posibles categorías. A continuación, puede utilizar técnicas integradas de transformación de datos reversibles

o irreversibles, como la sustitución, el cifrado y el descifrado, todo ello sin necesidad de escribir ningún código. A continuación, puede utilizar los conjuntos de datos limpios y enmascarados en un momento posterior para realizar tareas de análisis, elaboración de informes y aprendizaje automático. Algunas de las técnicas de enmascaramiento de datos disponibles en incluyen: DataBrew

- Procesamiento de hash: aplique funciones de hash a los valores de las columnas.
- Sustitución: sustituye los datos personales por otros valores que parezcan auténticos.
- Anulación o eliminación: sustituye un campo concreto por un valor nulo o elimina la columna.
- Enmascaramiento: utilice la codificación de caracteres o oculte determinadas partes de las columnas.

Las siguientes son las técnicas de cifrado disponibles:

- Cifrado determinista: aplique algoritmos de cifrado determinista a los valores de las columnas. El cifrado determinista siempre produce el mismo texto cifrado para un valor.
- Cifrado probabilístico: aplique algoritmos de cifrado probabilístico a los valores de las columnas. El cifrado probabilístico produce un texto cifrado diferente cada vez que se aplica.

Para obtener una lista completa de las recetas de transformación de datos personales proporcionadas en DataBrew, consulte los pasos básicos de la información de identificación personal (PII).

AWS Glue Calidad de los datos

AWS Glue La calidad de los datos le ayuda a automatizar y poner en funcionamiento la entrega de datos de alta calidad en todas las canalizaciones de datos, de forma proactiva, antes de entregarlos a sus consumidores de datos. AWS Glue Data Quality proporciona un análisis estadístico de los problemas de calidad de los datos en todos sus flujos de datos, puede activar alertas en Amazon EventBridge y puede hacer recomendaciones de normas de calidad para su corrección. AWS Glue Data Quality también admite la creación de reglas con un lenguaje específico del dominio para que pueda crear reglas de calidad de datos personalizadas.

AWS Key Management Service

AWS Key Management Service (AWS KMS) le ayuda a crear y controlar claves criptográficas para proteger sus datos. AWS KMS utiliza módulos de seguridad de hardware para proteger y validar

AWS KMS keys en el marco del programa de validación de módulos criptográficos FIPS 140-2. Para obtener más información sobre cómo se utiliza este servicio en un contexto de seguridad, consulte la arquitectura de referencia de AWS seguridad.

AWS KMS se integra con la mayoría de los sistemas Servicios de AWS que ofrecen cifrado, y puede utilizar claves KMS en las aplicaciones que procesan y almacenan datos personales. Puede utilizarlas AWS KMS para cumplir diversos requisitos de privacidad y proteger los datos personales, como:

- Uso de claves gestionadas por el cliente para tener un mayor control sobre la resistencia, la rotación, la caducidad y otras opciones.
- Uso de claves exclusivas administradas por el cliente para proteger los datos personales y los secretos que permiten el acceso a los datos personales.
- Definir los niveles de clasificación de datos y designar al menos una clave dedicada gestionada por el cliente por nivel. Por ejemplo, puede tener una clave para cifrar los datos operativos y otra para cifrar los datos personales.
- Impedir el acceso involuntario entre cuentas a las claves de KMS.
- Almacenar las claves de KMS en el mismo lugar Cuenta de AWS que el recurso que se va a cifrar.
- Implementar la separación de tareas para la administración y el uso de las claves de KMS. Para obtener más información, consulte Cómo usar KMS e IAM para habilitar controles de seguridad independientes para los datos cifrados en S3 (entrada del AWS blog).
- Impulsar la rotación automática de las llaves mediante barandillas preventivas y reactivas.

De forma predeterminada, las claves KMS se almacenan y solo se pueden usar en la región en la que se crearon. Si su organización tiene requisitos específicos de residencia y soberanía de los datos, considere si las claves KMS multirregionales son adecuadas para su caso de uso. Las claves multirregionales son claves KMS de uso especial en diferentes formatos Regiones de AWS que se pueden usar indistintamente. El proceso de creación de una clave multirregional traslada el material clave más allá de las Región de AWS fronteras internas AWS KMS, por lo que esta falta de aislamiento regional podría no ser compatible con los objetivos de cumplimiento de la organización. Una forma de solucionar este problema consiste en utilizar un tipo diferente de clave de KMS, como una clave gestionada por el cliente para una región específica.

AWS Zonas Locales

Si necesita cumplir con los requisitos de residencia de los datos, puede implementar recursos que almacenen y procesen datos personales de forma específica Regiones de AWS para cumplir con estos requisitos. También puede usar Zonas AWS Locales, que le ayudan a ubicar recursos informáticos, de almacenamiento, de bases de datos y otros AWS recursos selectos cerca de grandes centros industriales y de población. Una zona local es una extensión de una Región de AWS que se encuentra cerca geográficamente de una gran área metropolitana. Puede colocar tipos específicos de recursos dentro de una zona local, cerca de la región a la que corresponde la zona local. Las Zonas Locales pueden ayudarlo a cumplir con los requisitos de residencia de datos cuando una región no esté disponible dentro de la misma jurisdicción legal. Cuando utilice Zonas Locales, tenga en cuenta los controles de residencia de datos que se implementan en su organización. Por ejemplo, es posible que necesite un control para evitar la transferencia de datos de una zona local específica a otra región. Para obtener más información sobre cómo SCPs mantener las barreras de transferencia de datos transfronterizas, consulte Mejores prácticas para gestionar la residencia de datos en Zonas AWS Locales mediante controles de zona de aterrizaje (entrada del AWS blog).

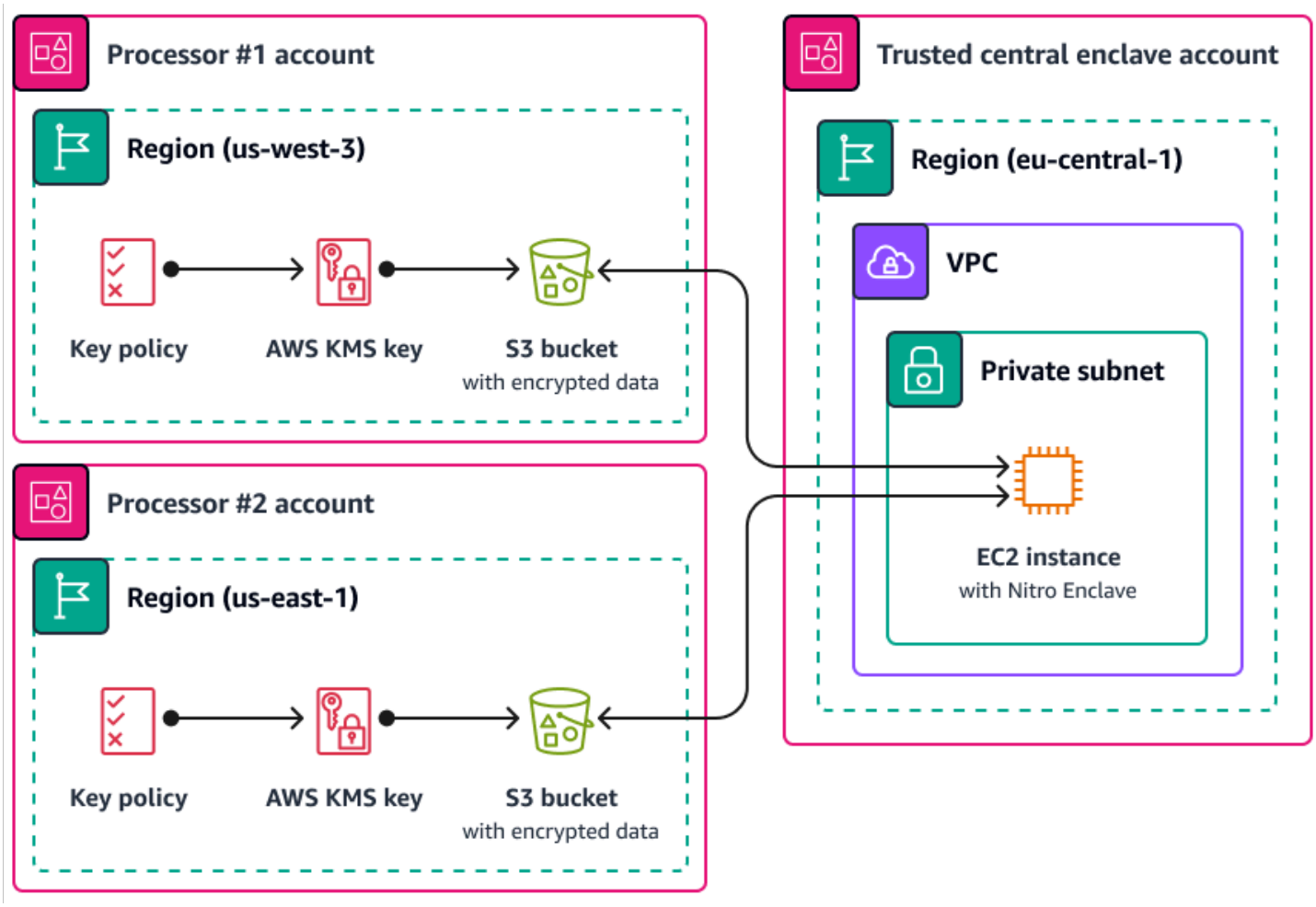
AWS Nitro Enclaves

Considere su estrategia de segmentación de datos desde una perspectiva de procesamiento, como el procesamiento de datos personales con un servicio informático como Amazon Elastic Compute Cloud (Amazon EC2). La computación confidencial, como parte de una estrategia de arquitectura más amplia, puede ayudarlo a aislar el procesamiento de datos personales en un enclave de CPU aislado, protegido y confiable. Los enclaves son máquinas virtuales independientes, reforzadas y muy restringidas. AWS Nitro Enclaves es una EC2 función de Amazon que puede ayudarte a crear estos entornos informáticos aislados. Para obtener más información, consulte El diseño de seguridad del sistema AWS Nitro (AWS documento técnico).

Nitro Enclaves despliega un núcleo que está separado del núcleo de la instancia principal. El núcleo de la instancia principal no tiene acceso al enclave. Los usuarios no pueden acceder mediante SSH ni de forma remota a los datos y las aplicaciones del enclave. Las aplicaciones que procesan datos personales pueden integrarse en el enclave y configurarse para usar el Vsock del enclave, el socket que facilita la comunicación entre el enclave y la instancia principal.

Un caso de uso en el que Nitro Enclaves puede resultar útil es el procesamiento conjunto entre dos procesadores de datos que están separados Regiones de AWS y que podrían no confiar entre sí. La siguiente imagen muestra cómo se puede utilizar un enclave para el procesamiento centralizado, una clave KMS para cifrar los datos personales antes de enviarlos al enclave y una AWS KMS

key política que compruebe que el enclave que solicita el descifrado tiene las medidas únicas en su documento de certificación. Para obtener más información e instrucciones, consulte Uso de la atestación criptográfica con. AWS KMS Para ver un ejemplo de política de claves, consulta Exija una certificación para usar una clave AWS KMS esta guía.



Con esta implementación, solo los procesadores de datos respectivos y el enclave subyacente tienen acceso a los datos personales en texto plano. El único lugar donde están expuestos los datos, fuera del entorno de los respectivos procesadores de datos, es en el propio enclave, que está diseñado para evitar el acceso y la manipulación.

AWS PrivateLink

Muchas organizaciones desean limitar la exposición de los datos personales a redes que no son de confianza. Por ejemplo, si desea mejorar la privacidad del diseño general de la arquitectura de la aplicación, puede segmentar las redes en función de la confidencialidad de los datos (de forma similar a la separación lógica y física de los conjuntos de datos que se analiza en la Servicios y

características de AWS que ayudan a segmentar los datos sección). AWS PrivateLinkle ayuda a crear conexiones unidireccionales y privadas desde sus nubes privadas virtuales (VPCs) a servicios externos a la VPC. Con AWS PrivateLinkél, puede configurar conexiones privadas dedicadas a los servicios que almacenan o procesan datos personales en su entorno; no es necesario conectarse a puntos finales públicos ni transferir estos datos a través de redes públicas que no sean de confianza. Al habilitar los puntos finales de AWS PrivateLink servicio para los servicios incluidos, no se necesita una pasarela de Internet, un dispositivo NAT, una dirección IP pública, una AWS Direct Connect conexión o una conexión para AWS Site-to-Site VPN comunicarse. Cuando te conectas AWS PrivateLink a un servicio que proporciona acceso a datos personales, puedes usar políticas de puntos finales de VPC y grupos de seguridad para controlar el acceso, de acuerdo con la definición del perímetro de datos de tu organización. Para ver un ejemplo de política de puntos finales de VPC que permite que solo los principios y AWS recursos de IAM de una organización de confianza accedan a un punto final de servicio, consulte Exija ser miembro de una organización para acceder a los recursos de VPC esta guía.

AWS Resource Access Manager

AWS Resource Access Manager (AWS RAM) le ayuda a compartir sus recursos de forma segura Cuentas de AWS para reducir la sobrecarga operativa y ofrecer visibilidad y auditabilidad. Cuando planifique su estrategia de segmentación de varias cuentas, considere la posibilidad de AWS RAM compartir los almacenes de datos personales que almacene en una cuenta separada y aislada. Puedes compartir esos datos personales con otras cuentas de confianza con el fin de procesarlos. En AWS RAM, puedes administrar los permisos que definen qué acciones se pueden realizar en los recursos compartidos. AWS RAM Se ha iniciado sesión en todas las llamadas a la API CloudTrail. Además, puede configurar Amazon CloudWatch Events para que le notifique automáticamente eventos específicos en AWS RAM, por ejemplo, cuando se realicen cambios en un recurso compartido.

Si bien puede compartir muchos tipos de AWS recursos con otros Cuentas de AWS mediante políticas basadas en recursos en IAM o políticas de bucket en Amazon S3, AWS RAM ofrece varios beneficios adicionales en materia de privacidad. AWS proporciona a los propietarios de los datos una visibilidad adicional sobre cómo y con quién se comparten los datos en su Cuentas de AWS empresa, lo que incluye:

- Poder compartir un recurso con una unidad organizativa completa en lugar de actualizar manualmente las listas de cuentas IDs
- Hacer cumplir el proceso de invitación para iniciar acciones si la cuenta de consumidor no forma parte de su organización

- Visibilidad de los directores de IAM específicos que tienen acceso a cada recurso individual

Si ha utilizado anteriormente una política basada en recursos para gestionar un recurso compartido y desea utilizarla en AWS RAM su lugar, utilice la operación de API. PromoteResourceShareCreatedFromPolicy

Amazon SageMaker AI

Amazon SageMaker AI es un servicio de aprendizaje automático (ML) gestionado que le ayuda a crear y entrenar modelos de aprendizaje automático y, a continuación, a implementarlos en un entorno hospedado listo para la producción. SageMaker La IA está diseñada para facilitar la preparación de los datos de entrenamiento y la creación de características de los modelos.

Monitor de modelos Amazon SageMaker AI

Muchas organizaciones consideran la desviación de datos a la hora de entrenar modelos de aprendizaje automático. La desviación de datos es una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de aprendizaje automático, 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. Si la naturaleza estadística de los datos que recibe un modelo de aprendizaje automático durante la producción se aleja de la naturaleza de los datos de referencia en los que se entrenó, la precisión de las predicciones podría disminuir. Amazon SageMaker AI Model Monitor puede monitorear continuamente la calidad de los modelos de aprendizaje automático de Amazon SageMaker AI en producción y monitorear la calidad de los datos. La detección temprana y proactiva de la desviación de datos puede ayudarle a implementar acciones correctivas, como volver a capacitar los modelos, auditar los sistemas iniciales o solucionar problemas de calidad de los datos. Model Monitor puede reducir la necesidad de monitorizar manualmente los modelos o crear herramientas adicionales.

Amazon SageMaker AI Clarify

Amazon SageMaker AI Clarify proporciona información sobre el sesgo y la explicabilidad del modelo. SageMaker AI Clarify se suele utilizar durante la preparación de los datos del modelo de aprendizaje automático y durante la fase general de desarrollo. Los desarrolladores pueden especificar los atributos de interés, como el sexo o la edad, y SageMaker AI Clarify ejecuta un conjunto de algoritmos para detectar cualquier presencia de sesgo en esos atributos. Una vez ejecutado el algoritmo, SageMaker AI Clarify proporciona un informe visual con una descripción de las fuentes y las medidas del posible sesgo para que puedas identificar las medidas necesarias

para subsanarlo. Por ejemplo, en un conjunto de datos financieros que contenga solo unos pocos ejemplos de préstamos empresariales concedidos a un grupo de edad en comparación con otros, SageMaker podría detectar desequilibrios para evitar un modelo que desfavorezca a ese grupo de edad. También puede comprobar si los modelos ya entrenados están sesgados revisando sus predicciones y supervisando continuamente esos modelos de aprendizaje automático para detectar sesgos. Por último, SageMaker AI Clarify está integrado con Amazon SageMaker AI Experiments para proporcionar un gráfico que explica qué características contribuyeron más al proceso general de elaboración de predicciones de un modelo. Esta información podría ser útil para obtener resultados de explicabilidad y podría ayudarle a determinar si una entrada determinada del modelo tiene más influencia de la que debería en el comportamiento general del modelo.

Tarjeta SageMaker modelo Amazon

Amazon SageMaker Model Card puede ayudarle a documentar detalles importantes sobre sus modelos de aprendizaje automático con fines de gobernanza y elaboración de informes. Estos detalles pueden incluir el propietario del modelo, el propósito general, los casos de uso previstos, las suposiciones asumidas, la calificación de riesgo de un modelo, los detalles y métricas de la capacitación y los resultados de la evaluación. Para obtener más información, consulte Model Explainability with AWS Artificial Intelligence and Machine Learning Solutions (documentoAWS técnico).

AWS funciones que ayudan a gestionar el ciclo de vida de los datos

Cuando los datos personales ya no sean necesarios, puede utilizar el ciclo de vida y time-to-live las políticas para los datos de muchos almacenes de datos diferentes. Al configurar las políticas de retención de datos, tenga en cuenta las siguientes ubicaciones que podrían contener datos personales:

- Bases de datos, como Amazon DynamoDB y Amazon Relational Database Service (Amazon RDS)
- Buckets de Amazon S3
- Inicia sesión desde y CloudWatch CloudTrail
- Datos en caché de migraciones en AWS Database Migration Service (AWS DMS) y proyectos AWS Glue DataBrew
- Copias de seguridad e instantáneas

Las siguientes funciones Servicios de AWS y las siguientes pueden ayudarle a configurar las políticas de retención de datos en sus AWS entornos:

- Amazon S3 Lifecycle: conjunto de reglas que definen las acciones que Amazon S3 aplica a un grupo de objetos. En la configuración del ciclo de vida de Amazon S3, puede crear acciones de caducidad, que definen cuándo Amazon S3 elimina los objetos caducados en su nombre. Para obtener más información, consulte Administración del ciclo de vida del almacenamiento.
- Amazon Data Lifecycle Manager: en Amazon EC2, cree una política que automatice la creación, retención y eliminación de las instantáneas de Amazon Elastic Block Store (Amazon EBS) y de las Amazon Machine Images respaldadas por EBS (). AMIs
- DynamoDB Time to Live (TTL): defina una marca de tiempo por elemento que determine cuándo un elemento ya no es necesario. Poco después de la fecha y hora de la marca de tiempo especificada, DynamoDB elimina el elemento de la tabla.
- Configuración de retención de CloudWatch registros en los registros: puede ajustar la política de retención de cada grupo de registros a un valor comprendido entre 1 día y 10 años.
- AWS Backup— Implemente políticas de protección de datos de forma centralizada para configurar, administrar y gobernar su actividad de respaldo en una variedad de AWS recursos, incluidos los buckets S3, las instancias de bases de datos de RDS, las tablas de DynamoDB, los volúmenes de EBS y muchos más. Aplique políticas de respaldo a sus AWS recursos especificando los tipos de recursos o proporcionando una granularidad adicional al aplicarlas en función de las etiquetas de recursos existentes. Audite e informe sobre la actividad de respaldo desde una consola centralizada para cumplir con los requisitos de cumplimiento de las normas de respaldo.

Servicios y características de AWS que ayudan a segmentar los datos

La segmentación de datos es el proceso mediante el cual se almacenan los datos en contenedores separados. Esto puede ayudarle a proporcionar medidas de seguridad y autenticación diferenciadas para cada conjunto de datos y a reducir el alcance del impacto de la exposición en todo el conjunto de datos. Por ejemplo, en lugar de almacenar todos los datos de los clientes en una base de datos grande, puede segmentar estos datos en grupos más pequeños y fáciles de administrar.

Puede utilizar la separación física y lógica para segmentar los datos personales:

- Separación física: el acto de almacenar los datos en almacenes de datos separados o de distribuirlos en AWS recursos separados. Si bien los datos están separados físicamente, es posible que los mismos directores puedan acceder a ambos recursos. Por eso recomendamos combinar la separación física con la separación lógica.
- Separación lógica: acto de aislar los datos mediante controles de acceso. Las diferentes funciones laborales requieren diferentes niveles de acceso a subconjuntos de datos personales. Para ver

un ejemplo de política que implementa la separación lógica, consulte Otorgue acceso a atributos específicos de Amazon DynamoDB esta guía.

La combinación de una separación lógica y física proporciona flexibilidad, simplicidad y granularidad a la hora de redactar políticas basadas en la identidad y en los recursos para respaldar el acceso diferenciado entre las distintas funciones laborales. Por ejemplo, puede resultar complejo desde el punto de vista operativo crear políticas que separen de forma lógica las diferentes clasificaciones de datos en un único depósito de S3. El uso de depósitos de S3 dedicados para cada clasificación de datos simplifica la configuración y la administración de las políticas.

Ejemplos de políticas relacionadas con la privacidad

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

Muchas organizaciones que manejan datos confidenciales adoptan un enfoque preventivo, con niveles de controles reactivos y de detección implementados en todas partes. En esta sección se proporcionan ejemplos de políticas relacionadas con la privacidad para AWS Identity and Access Management (IAM) y (). AWS Organizations AWS Key Management Service AWS KMS Estas políticas pueden ayudar a su organización a cumplir diversos objetivos de privacidad relacionados con el uso, la limitación de la divulgación y la transferencia transfronteriza de datos mediante un enfoque preventivo. Muchas de estas políticas se mencionan en las secciones anteriores de esta guía.

Esta sección contiene los siguientes ejemplos de políticas:

- Exija el acceso desde direcciones IP específicas
- Exija ser miembro de una organización para acceder a los recursos de VPC
- Restrinja las transferencias de datos entre Regiones de AWS
- Otorgue acceso a atributos específicos de Amazon DynamoDB
- Restringir los cambios en las configuraciones de VPC
- Exija una certificación para usar una clave AWS KMS

Exija el acceso desde direcciones IP específicas

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

Esta política permite al `john_stiles` usuario asumir funciones de IAM solo si la llamada proviene de una dirección IP dentro de los rangos `192.0.2.0/24` o`203.0.113.0/24`. Esta política puede ayudar a evitar la divulgación no intencionada de datos personales y las transferencias de datos transfronterizas no deseadas. Por ejemplo, si su organización cuenta con personal de atención al cliente que necesita acceder a datos personales, es posible que desee que ese personal solo

acceda a esos datos desde las oficinas que estén ubicadas en un subconjunto de áreas específicas. Regiones de AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

Exija ser miembro de una organización para acceder a los recursos de VPC

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

Esta política de puntos de conexión de VPC permite que solo los directores y recursos AWS Identity and Access Management (IAM) de la `o-1abcde123` organización accedan a los puntos de enlace

de Amazon Personalize (Amazon S3). Este control preventivo ayuda a establecer una zona de confianza y a definir el perímetro de los datos personales. Para obtener más información sobre cómo esta política puede ayudar a proteger la privacidad y los datos personales en su organización, consulte AWS PrivateLink esta guía.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowOnlyIntendedResourcesAndPrincipals",
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "o-1abcde123",
                    "aws:ResourceOrgID": "o-1abcde123"
                }
            }
        }
    ]
}
```

Restrinja las transferencias de datos entre Regiones de AWS

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

Con la excepción de dos funciones AWS Identity and Access Management (IAM), esta política de control de servicios deniega las llamadas a la API a regiones Servicios de AWS Regiones de AWS distintas de `eu-west-1` y`eu-central-1`. Este SCP puede ayudar a evitar la creación de servicios de AWS almacenamiento y procesamiento en regiones no aprobadas. Esto puede ayudar a evitar que los datos personales sean manejados por completo Servicios de AWS en esas regiones. Esta política utiliza un `NotAction` parámetro porque tiene en cuenta los servicios globales de AWS, como IAM, y los servicios que se integran con los servicios globales, como AWS Key Management Service (AWS KMS) y Amazon CloudFront. En los valores de los parámetros, puede especificar esos servicios globales y otros servicios no aplicables como excepciones. Para obtener más información

sobre cómo esta política puede ayudar a proteger la privacidad y los datos personales de su organización, consulte AWS Organizations esta guía.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "chime:*",
                "cloudfront:*",
                "config:*",
                "cur:*",
                "directconnect:*",
                "ec2:DescribeRegions",
                "ec2:DescribeTransitGateways",
                "ec2:DescribeVpnGateways",
                "fms:*",
                "globalaccelerator:*",
                "health:*",
                "iam:*",
                "importexport:*",
                "kms:*",
                "mobileanalytics:*",
                "networkmanager:*",
                "organizations:*",
                "pricing:*",
                "route53:*",
                "route53domains:*",
                "route53-recovery-cluster:*",
                "route53-recovery-control-config:*",
                "route53-recovery-readiness:*",
                "s3:GetAccountPublic*",
                "s3:ListAllMyBuckets",
                "s3:ListMultiRegionAccessPoints",
```

```
                "s3:PutAccountPublic*",
                "shield:*",
                "sts:*",
                "support:*",
                "trustedadvisor:*",
                "waf-regional:*",
                "waf:*",
                "wafv2:*",
                "wellarchitected:*"
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:RequestedRegion": [
                        "eu-central-1",
                        "eu-west-1"
                    ]
                },
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
    ]
}
```

Otorgue acceso a atributos específicos de Amazon DynamoDB

Nos encantaría saber de usted. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

A medida que su organización analice las estrategias para separar física y lógicamente los datos personales, considere qué servicios AWS de almacenamiento respaldan políticas de control de acceso detalladas (IAM). AWS Identity and Access Management La siguiente política basada en la identidad permite recuperar únicamente los `LastLoggedIn` atributos `UserIDSignUpTime`, y de una tabla de Amazon DynamoDB denominada. `Users` Por ejemplo, puede adjuntar esta política a un rol de atención al cliente en lugar de darle acceso a este rol a todo el conjunto de datos personal.

Para obtener más información sobre cómo esta política puede ayudar a proteger la privacidad y los datos personales en su organización, consulte Servicios y características de AWS que ayudan a segmentar los datos esta guía.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan",
            "dynamodb:TransactGetItems"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
         "Condition":{
            "ForAllValues:StringEquals":{
               "dynamodb:Attributes":[
                  "UserID",
                  "SignUpTime",
                  "LastLoggedIn"
               ]
            },
            "StringEquals":{
               "dynanamodb:Select":[
                  "SPECIFIC_ATTRIBUTES"
               ]
            }
         }
      }
   ]
}
```

Restringir los cambios en las configuraciones de VPC

Nos encantaría saber de usted. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

Una vez que haya diseñado e implementado la AWS infraestructura que cumple con sus requisitos de transferencia de datos transfronteriza, que incluye los flujos de datos de red, es posible que desee evitar las modificaciones. La siguiente política de control de servicios ayuda a evitar desviaciones o modificaciones no intencionadas en la configuración de la VPC. Rechaza los nuevos adjuntos de las puertas de enlace de Internet, las conexiones de emparejamiento de VPC, los archivos adjuntos de las pasarelas de tránsito y las nuevas conexiones de VPN. Para obtener más información sobre cómo esta política puede ayudar a proteger la privacidad y los datos personales de su organización, consulte esta AWS Transit Gateway guía.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "ec2:AttachEgressOnlyInternetGateway",
                "ec2:CreateVpcPeeringConnection",
                "ec2:AcceptVpcPeeringConnection",
                "ec2:CreateVpc",
                "ec2:CreateSubnet",
                "ec2:CreateRouteTable",
                "ec2:CreateRoute",
                "ec2:AssociateRouteTable",
                "ec2:ModifyVpcAttribute",
                "ec2:*TransitGateway",
                "ec2:*TransitGateway*",
                "globalaccelerator:Create*",
                "globalaccelerator:Update*"

            ],
            "Resource": "*",
            "Effect": "Deny",
            "Condition": {
                "ArnNotLike": {
                    "aws:PrincipalARN": [
                        "arn:aws:iam::*:role/Role1AllowedToBypassThisSCP",
                        "arn:aws:iam::*:role/Role2AllowedToBypassThisSCP"
                    ]
                }
            }
        }
```

```
    ]
}
```

Exija una certificación para usar una clave AWS KMS

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

La siguiente política clave AWS Key Management Service (AWS KMS) permite a las instancias de AWS Nitro Enclave utilizar una clave KMS solo si el documento de certificación del enclave que figura en la solicitud coincide con las medidas de la declaración de estado. Esta política permite que solo los enclaves de confianza descifren los datos. Para obtener más información sobre cómo esta política puede ayudar a proteger la privacidad y los datos personales de su organización, consulte esta AWS Nitro Enclaves guía. Para obtener una lista completa de las claves de AWS KMS condición que se pueden utilizar en las políticas clave y en las políticas AWS Identity and Access Management (de IAM), consulte las claves de condición de AWS KMS.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Enable enclave data processing",
         "Effect": "Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:role/data-processing"
         },
         "Action": [
            "kms:Decrypt",
            "kms:GenerateDataKey",
            "kms:GenerateRandom"
         ],
         "Resource": "*",
         "Condition": {
            "StringEqualsIgnoreCase": {
               "kms:RecipientAttestation:ImageSha384":
 "EXAMPLE8abcdef7abcdef6abcdef5abcdef4abcdef3abcdef2abcdef1abcdef1abcdef0abcdef1abcdEXAMPLE",
               "kms:RecipientAttestation:PCR0":
 "EXAMPLEbc2ecbb68ed99a13d7122abfc0666b926a79d5379bc58b9445c84217f59cfdd36c08b2c79552928702EXAM
```

```
                "kms:RecipientAttestation:PCR1":
  "EXAMPLE050abf6b993c915505f3220e2d82b51aff830ad14cbecc2eec1bf0b4ae749d311c663f464cde9f718aEXAM
                "kms:RecipientAttestation:PCR2":
  "EXAMPLEc300289e872e6ac4d19b0b5ac4a9b020c98295643ff3978610750ce6a86f7edff24e3c0a4a445f2ff8EXAM
                "kms:RecipientAttestation:PCR3":
  "EXAMPLE11de9baee597508183477f097ae385d4a2c885aa655432365b53b812694e230bbe8e1bb1b8de748fe1EXAM
                "kms:RecipientAttestation:PCR4":
  "EXAMPLE6b9b3d89a53b13f5dfd14a1049ec0b80a9ae4b159adde479e9f7f512f33e835a0b9023ca51ada02160EXAM
                "kms:RecipientAttestation:PCR8":
  "EXAMPLE34a884328944cd806127c7784677ab60a154249fd21546a217299ccfa1ebfe4fa96a163bf41d3bcfaeEXAM
            }
         }
      }
   ]
}
```

Recursos

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

AWS Guía prescriptiva

- AWS Arquitectura de referencia de seguridad (AWS SRA)

AWS documentación

- Protección de datos (AWS Well-Architected Framework)
- Clasificación de datos (documento técnico)AWS
- Amazon Web Services: Riesgo y conformidad (AWS documento técnico)
- Arquitecturas híbridas para abordar los requisitos de procesamiento de datos personales (documento técnico)AWS
- Cómo navegar por el cumplimiento del RGPD (documento técnico) AWSAWS
- Cómo crear un perímetro de datos (documento técnico) AWSAWS
- AWS Documentación de seguridad

Otros AWS recursos

- AWS Programas de cumplimiento
- AWS Modelo de responsabilidad compartida
- Preguntas frecuentes sobre privacidad de datos
- AWS Servicios de garantía de seguridad
- AWS Compromiso de soberanía digital: control sin concesiones (AWS entrada del blog)
- AWS Aprendizaje sobre seguridad

Colaboradores

Nos encantaría saber de ti. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

El autor de esta guía es el equipo de los Servicios AWS de Garantía de Seguridad. Si necesita ayuda para implementar las recomendaciones de esta guía y poner en funcionamiento sus cargas de trabajo, póngase en contacto con el equipo de los Servicios de Garantía AWS de Seguridad.

Autores principales

- Daniel Nieters, consultor principal de privacidad AWS
- Amber Welch, AWS consultora sénior de privacidad
- Robert Carter, director del programa AWS técnico

Colaboradores

- Avik Mukherjee, consultor sénior de seguridad AWS
- David Bounds, arquitecto sénior de soluciones AWS
- Jeff Lombardo, arquitecto AWS sénior de soluciones de seguridad
- Ram Ramani, arquitecto AWS principal de soluciones de seguridad
- Vanessa Jacobs, AWS consultora sénior de seguridad

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
Actualizaciones importantes	Hicimos actualizaciones importantes en todo momento.	26 de marzo de 2024
Publicación inicial	—	2 de octubre de 2023

AWS Glosario de orientación prescriptiva

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

Números

Las 7 R

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

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

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

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

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

migración activa-pasiva

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

función agregada

Función SQL que opera en un grupo de filas y calcula un único valor de retorno para el grupo. Algunos ejemplos de funciones agregadas incluyen `SUM` y`MAX`.

IA

Véase inteligencia artificial.

AIOps

Consulte las operaciones de inteligencia artificial.

anonimización

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

antipatrones

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

control de aplicaciones

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

cartera de aplicaciones

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

inteligencia artificial (IA)

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

operaciones de inteligencia artificial (AIOps)

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

cifrado asimétrico

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

atomicidad, consistencia, aislamiento, durabilidad (ACID)

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

control de acceso basado en atributos (ABAC)

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

origen de datos fidedigno

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

Zona de disponibilidad

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

AWS Marco de adopción de la nube (AWS CAF)

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

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

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

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

B

Un bot malo

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

BCP

Consulte la planificación de la continuidad del negocio.

gráfico de comportamiento

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

sistema big-endian

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

clasificación binaria

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

filtro de floración

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

implementación azul/verde

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

bot

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

botnet

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

branch

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

acceso con cristales rotos

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

estrategia de implementación sobre infraestructura existente

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

caché de búfer

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

capacidad empresarial

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

planificación de la continuidad del negocio (BCP)

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

C

CAF

Consulte el marco AWS de adopción de la nube.

despliegue canario

El lanzamiento lento e incremental de una versión para los usuarios finales. Cuando 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.

captura de datos de cambio (CDC)

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

ingeniería del caos

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

CI/CD

Consulte la integración continua y la entrega continua.

clasificación

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

cifrado del cliente

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

Centro de excelencia en la nube (CCoE)

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

computación en la nube

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

modelo operativo en la nube

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

etapas de adopción de la nube

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

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir una CCo E, establecer un modelo de operaciones)
- Migración: migración de aplicaciones individuales
- Reinvención: optimización de productos y servicios e innovación en la nube

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

CMDB

Consulte la base de datos de administración de la configuración.

repositorio de código

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

caché en frío

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

datos fríos

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

visión artificial (CV)

Campo de la IA que utiliza el aprendizaje automático para analizar y extraer información de formatos visuales, como imágenes y vídeos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

desviación de configuración

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

base de datos de administración de configuración (CMDB)

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

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

paquete de conformidad

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

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD is commonly described as a pipeline. CI/CDpuede 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

Vea la visión artificial.

D

datos en reposo

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

clasificación de datos

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

desviación de datos

Una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de machine learning, o un cambio significativo en los datos de entrada

a lo largo del tiempo. La desviación de los datos puede reducir la calidad, la precisión y la imparcialidad generales de las predicciones de los modelos de machine learning.

datos en tránsito

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

malla de datos

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

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de datos (DDL)

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

lenguaje de manipulación de datos (DML)

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

DDL

Consulte el lenguaje de definición de bases de datos.

conjunto profundo

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

aprendizaje profundo

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

defense-in-depth

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

administrador delegado

En AWS Organizations, un servicio compatible puede registrar una cuenta de AWS miembro para administrar las cuentas de la organización y gestionar los permisos de ese servicio. Esta cuenta se denomina administrador delegado para ese servicio. Para obtener más información y una lista de servicios compatibles, consulte Servicios que funcionan con AWS Organizations en la documentación de AWS Organizations .

Implementación

El proceso de hacer que una aplicación, características nuevas o correcciones de código se encuentren disponibles en el entorno de destino. La implementación abarca implementar

cambios en una base de código y, a continuación, crear y ejecutar esa base en los entornos de la aplicación.

entorno de desarrollo

Consulte entorno.

control de detección

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

asignación de flujos de valor para el desarrollo (DVSM)

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

gemelo digital

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

tabla de dimensiones

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

desastre

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

recuperación de desastres (DR)

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

DML

Consulte el lenguaje de manipulación de bases de datos.

diseño basado en el dominio

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

DR

Consulte recuperación ante desastres.

detección de deriva

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

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

EDI

Véase intercambio electrónico de datos.

computación en la periferia

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

intercambio electrónico de datos (EDI)

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

cifrado

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

clave de cifrado

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

endianidad

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

punto de conexión

Consulte el punto final del servicio.

servicio de punto de conexión

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

planificación de recursos empresariales (ERP)

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

cifrado de sobre

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

entorno

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

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

epopeya

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

ERP

Consulte planificación de recursos empresariales.

análisis de datos de tipo exploratorio (EDA)

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

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

F

tabla de datos

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

fallan rápidamente

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

límite de aislamiento de fallas

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

rama de característica

Consulte la sucursal.

características

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

importancia de las características

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

transformación de funciones

Optimizar los datos para el proceso de ML, lo que incluye enriquecer los datos con fuentes adicionales, escalar los valores o extraer varios conjuntos de información de un solo campo de datos. Esto permite que el modelo de ML se beneficie de los datos. Por ejemplo, si divide la fecha del “27 de mayo de 2021 00:15:37” en “jueves”, “mayo”, “2021” y “15”, puede ayudar al algoritmo de aprendizaje a aprender patrones matizados asociados a los diferentes componentes de los datos.

indicaciones de unos pocos pasos

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

FGAC

Consulte el control de acceso detallado.

control de acceso preciso (FGAC)

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

migración relámpago

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

FM

Consulte el modelo básico.

modelo de base (FM)

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

G

IA generativa

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

bloqueo geográfico

Consulta las restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

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

Flujo de trabajo de Gitflow

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

imagen dorada

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

estrategia de implementación desde cero

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

barrera de protección

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

H

HA

Consulte la alta disponibilidad.

migración heterogénea de bases de datos

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

alta disponibilidad (HA)

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

modernización histórica

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

datos retenidos

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

migración homogénea de bases de datos

Migración de la base de datos de origen a una base de datos de destino que comparte el mismo motor de base de datos (por ejemplo, Microsoft SQL Server a Amazon RDS para SQL Server). La migración homogénea suele formar parte de un esfuerzo para volver a alojar o redefinir la plataforma. Puede utilizar las utilidades de bases de datos nativas para migrar el esquema.

datos recientes

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

hotfix

Una solución urgente para un problema crítico en un entorno de producción. Debido a su urgencia, las revisiones suelen realizarse fuera del flujo de trabajo habitual de las versiones. DevOps

periodo de hiperatención

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

I

IaC

Vea la infraestructura como código.

políticas basadas en identidad

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

aplicación inactiva

Aplicación que utiliza un promedio de CPU y memoria de entre 5 y 20 por ciento durante un periodo de 90 días. En un proyecto de migración, es habitual retirar estas aplicaciones o mantenerlas en las instalaciones.

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

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

VPC entrante (de entrada)

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

migración gradual

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

Industria 4.0

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

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial (T) IIo

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

VPC de inspección

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

Internet de las cosas (IoT)

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

interpretabilidad

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

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

Conjunto de prácticas recomendadas para ofrecer servicios de TI y alinearlos con los requisitos empresariales. La ITIL proporciona la base para la ITSM.

administración de servicios de TI (ITSM)

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

ITIL

Consulte la biblioteca de información de TI.

ITSM

Consulte Administración de servicios de TI.

L

control de acceso basado en etiquetas (LBAC)

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

zona de aterrizaje

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

modelo de lenguaje grande (LLM)

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

migración grande

Migración de 300 servidores o más.

LBAC

Consulte control de acceso basado en etiquetas.

privilegio mínimo

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

migrar mediante lift-and-shift

Ver 7 Rs.

sistema little-endian

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

LLM

Véase un modelo de lenguaje amplio.

entornos inferiores

Véase entorno.

M

machine learning (ML)

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

rama principal

Ver sucursal.

malware

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

servicios gestionados

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

sistema de ejecución de fabricación (MES)

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

cuenta de miembro

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

MES

Consulte el sistema de ejecución de la fabricación.

Transporte telemétrico de Message Queue Queue (MQTT)

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

microservicio

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

arquitectura de microservicios

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

Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a compensar el costo inicial de las migraciones. El MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

migración a escala

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

fábrica de migración

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

metadatos de migración

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

patrón de migración

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

Migration Portfolio Assessment (MPA)

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

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

Evaluación de la preparación para la migración (MRA)

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

estrategia de migración

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

ML

Consulte el aprendizaje automático.

modernización

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

evaluación de la preparación para la modernización

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

aplicaciones monolíticas (monolitos)

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

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

MAPA

Consulte la evaluación de la cartera de migración.

MQTT

Consulte Message Queue Queue Telemetría y Transporte.

clasificación multiclase

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

infraestructura mutable

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

O

OAC

Consulte el control de acceso de origen.

OAI

Consulte la identidad de acceso de origen.

OCM

Consulte gestión del cambio organizacional.

migración fuera de línea

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

OI

Consulte integración de operaciones.

OLA

Véase el acuerdo a nivel operativo.

migración en línea

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

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

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

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

acuerdo de nivel operativo (OLA)

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

revisión de la preparación operativa (ORR)

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

tecnología operativa (OT)

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

integración de operaciones (OI)

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

registro de seguimiento organizativo

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

administración del cambio organizacional (OCM)

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

control de acceso de origen (OAC)

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

identidad de acceso de origen (OAI)

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

ORR

Consulte la revisión de la preparación operativa.

OT

Consulte la tecnología operativa.

VPC saliente (de salida)

En una arquitectura de AWS cuentas múltiples, una VPC que gestiona las conexiones de red que se inician desde una aplicación. La arquitectura AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

P

límite de permisos

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

información de identificación personal (PII)

Información que, vista directamente o combinada con otros datos relacionados, puede utilizarse para deducir de manera razonable la identidad de una persona. Algunos ejemplos de información de identificación personal son los nombres, las direcciones y la información de contacto.

PII

Consulte la información de identificación personal.

manual de estrategias

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

PLC

Consulte controlador lógico programable.

PLM

Consulte la gestión del ciclo de vida del producto.

policy

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

persistencia políglota

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

evaluación de cartera

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

predicate

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

pulsar un predicado

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

control preventivo

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

entidad principal

Una entidad AWS que puede realizar acciones y acceder a los recursos. Esta entidad suele ser un usuario raíz para un Cuenta de AWS rol de IAM o un usuario. Para obtener más información, consulte Entidad principal en Términos y conceptos de roles en la documentación de IAM.

privacidad desde el diseño

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

zonas alojadas privadas

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

control proactivo

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

gestión del ciclo de vida del producto (PLM)

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

entorno de producción

Consulte el entorno.

controlador lógico programable (PLC)

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

encadenamiento rápido

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

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

seudonimización

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

publish/subscribe (pub/sub)

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

Q

plan de consulta

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

regresión del plan de consulta

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

R

Matriz RACI

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

RAG

Consulte Retrieval Augmented Generation.

ransomware

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

Matriz RASCI

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

RCAC

Consulte control de acceso por filas y columnas.

réplica de lectura

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

rediseñar

Ver 7 Rs.

objetivo de punto de recuperación (RPO)

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

objetivo de tiempo de recuperación (RTO)

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

refactorizar

Ver 7 Rs.

Región

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

regresión

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

volver a alojar

Consulte 7 Rs.

versión

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

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

resiliencia

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

política basada en recursos

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

matriz responsable, confiable, consultada e informada (RACI)

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

control receptivo

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

retain

Consulte 7 Rs.

jubilarse

Ver 7 Rs.

Generación aumentada de recuperación (RAG)

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

rotación

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

control de acceso por filas y columnas (RCAC)

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

RPO

Consulte el objetivo del punto de recuperación.

RTO

Consulte el objetivo de tiempo de recuperación.

manual de procedimientos

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

S

SAML 2.0

Un estándar abierto que utilizan muchos proveedores de identidad (IdPs). Esta función permite el inicio de sesión único (SSO) federado, de modo que los usuarios pueden iniciar sesión AWS

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

SCADA

Consulte el control de supervisión y la adquisición de datos.

SCP

Consulte la política de control de servicios.

secreta

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

seguridad desde el diseño

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

control de seguridad

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

refuerzo de la seguridad

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

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

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

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

automatización de la respuesta de seguridad

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

cifrado del servidor

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

política de control de servicio (SCP)

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

punto de enlace de servicio

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

acuerdo de nivel de servicio (SLA)

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

indicador de nivel de servicio (SLI)

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

objetivo de nivel de servicio (SLO)

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

modelo de responsabilidad compartida

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

SIEM

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

punto único de fallo (SPOF)

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

SLA

Consulte el acuerdo de nivel de servicio.

SLI

Consulte el indicador de nivel de servicio.

SLO

Consulte el objetivo de nivel de servicio.

split-and-seed modelo

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

SPOF

Consulte el punto único de falla.

esquema en forma de estrella

Estructura organizativa de una base de datos que utiliza una tabla de hechos grande para almacenar datos medidos o transaccionales y una o más tablas dimensionales más pequeñas para almacenar los atributos de los datos. Esta estructura está diseñada para usarse en un almacén de datos o con fines de inteligencia empresarial.

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda desmantelar el sistema heredado. Este patrón utiliza la analogía de una higuera que crece hasta convertirse en un árbol estable y, finalmente, se apodera y reemplaza a su host. El patrón fue presentado por Martin Fowler como una forma de gestionar el riesgo al reescribir sistemas monolíticos. Para ver un ejemplo con la aplicación de este patrón, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

subred

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

supervisión, control y adquisición de datos (SCADA)

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

cifrado simétrico

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

pruebas sintéticas

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

indicador del sistema

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

T

etiquetas

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

variable de destino

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

lista de tareas

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

entorno de prueba

Consulte entorno.

entrenamiento

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

puerta de enlace de tránsito

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

flujo de trabajo basado en enlaces troncales

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

acceso de confianza

Otorgar permisos a un servicio que especifique para realizar tareas en su organización AWS Organizations y en sus cuentas en su nombre. El servicio de confianza crea un rol vinculado al servicio en cada cuenta, cuando ese rol es necesario, para realizar las tareas de administración

por usted. Para obtener más información, consulte AWS Organizations Utilización con otros AWS servicios en la AWS Organizations documentación.

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

tareas indiferenciadas

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

entornos superiores

Ver entorno.

V

succión

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

control de versión

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

Emparejamiento de VPC

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

vulnerabilidad

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

W

caché caliente

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

datos templados

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

función de ventana

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

carga de trabajo

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

flujo de trabajo

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

GUSANO

Mira, escribe una vez, lee muchas.

WQF

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

escribe una vez, lee muchas (WORM)

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

Z

ataque de día cero

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

vulnerabilidad de día cero

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

aviso de tiro cero

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

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

aplicación zombi

Aplicación que utiliza un promedio de CPU y memoria menor al 5 por ciento. En un proyecto de migración, es habitual retirar estas aplicaciones.

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