AWS Arquitectura de referencia de privacidad

AWS Orientación prescriptiva

AWS Orientación prescriptiva: AWS Arquitectura de referencia de privacidad

Table of Contents

Introducción 1
Avisos 1
Introducción 1
El modelo de responsabilidad AWS compartida y la privacidad 2
Entendiendo la AWS PRA 4
Uso de la AWS PRA y la SRA AWS 4
AWS Organizations y la estructura de cuentas dedicada 5
Operacionalización AWS de los servicios de privacidad 7
La arquitectura AWS de referencia de privacidad 9
Cuenta de administración de la organización 11
AWS Artifact 12
AWS Control Tower 13
AWS Organizations 14
UO de seguridad: cuenta de herramientas de seguridad 17
AWS CloudTrail 19
AWS Config 19
Amazon GuardDuty 21
Analizador de acceso de IAM 22
Amazon Macie 22
UO de seguridad: cuenta de archivos de registro 23
Almacenamiento de registros centralizado 24
Amazon Security Lake 26
Unidad organizativa de infraestructura: cuenta de red 26
Amazon CloudFront 29
AWS Resource Access Manager 29
AWS Transit Gateway 30
AWS WAF 31
UO de datos personales: cuenta de la aplicación de datos personales 32
Amazon Athena 35
Amazon Bedrock 36
AWS Clean Rooms 37
Amazon CloudWatch Logs 38
CodeGuru Revisor de Amazon 39
Amazon Comprehend 39

Amazon Data Firehose ... 40
Amazon DataZone ... 41
AWS Glue ... 41
AWS Key Management Service ... 44
AWS Lake Formation ... 45
Zonas locales de AWS ... 47
AWS Enclaves Nitro ... 47
AWS PrivateLink ... 48
AWS Resource Access Manager ... 49
Amazon SageMaker AI ... 50
AWS funciones que ayudan a gestionar el ciclo de vida de los datos ... 52
Servicios de AWS y funciones que ayudan a segmentar los datos ... 53
Servicios de AWS y funciones que ayudan a descubrir, clasificar o catalogar datos ... 54
Ejemplos de políticas relacionadas con la privacidad ... 55
Obligación del acceso desde direcciones IP específicas ... 55
Obligación de ser miembro de una organización para acceder a los recursos de VPC ... 57
Restrinja las transferencias de datos entre Regiones de AWS ... 58
Concesión de acceso a atributos específicos de Amazon DynamoDB ... 60
Restricción de la realización de cambios en las configuraciones de VPC ... 61
Exija una certificación para usar una clave AWS KMS ... 62
Preparación de estrategias para la expansión global ... 64
Zona de aterrizaje central con regiones administradas ... 65
Zonas de aterrizaje regionales ... 67
AWS Nube soberana europea ... 68
Recursos ... 70
Recomendaciones de AWS ... 70
AWSDocumentación de ... 70
Otros recursos de AWS ... 70
Colaboradores ... 71
Historial de documentos ... 72
Glosario ... 74
... 74
A ... 75
B ... 78
C ... 80
D ... 84

E 88
F 90
G 92
H 93
I 95
L 97
M 99
O 103
P 106
Q 109
R 109
S 112
T 116
U 118
V 119
W 119
Z 120
..... cxxii

AWS Arquitectura de referencia de privacidad

Amazon Web Services (colaboradores)

Septiembre de 2025 (historial del documento)

> **Encuesta**
>
> Nos encantaría saber su opinión. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

Avisos

Esta guía se suministra únicamente con fines informativos. No es un asesoramiento legal y no se debe confiar en él como 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 (AWS 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 la 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 compartida de AWS.

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 del cliente 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 administrar 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
- La forma en que define, almacena, rota y utiliza las claves criptográficas para el cifrado
- Quién y cuándo tiene acceso a sus datos, y cómo se conceden, 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 categoriza como infraestructura como servicio (IaaS). Por lo tanto, si utiliza Amazon EC2, debe realizar todas las tareas de configuración de la privacidad necesarias para los sistemas operativos invitados y para el software de aplicación o las utilidades que instale en las instancias de EC2. 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 administrar y clasificar los datos (contenido del cliente) y configurar las políticas utilizadas para acceder a los puntos de conexión con el fin de almacenar y recuperar los 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

> **Encuesta**
>
> Nos encantaría saber su opinión. 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 de cuentas dedicada
- Operacionalización AWS de los servicios de privacidad

Uso de la AWS PRA y la SRA AWS

> **Encuesta**
>
> Nos encantaría saber su opinión. 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 En esta guía únicamente se incluyen breves descripciones 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 básicas sobre la privacidad que puede ser útil tener en cuenta al principio de su traspaso a la Nube de AWS , ya que estas decisiones pueden afectar al diseño de la estructura de cuentas de la organización. Por ejemplo, estas son algunas de las preguntas que podría plantearse:

- ¿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 en la 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 mi organización para las transferencias de datos transfronterizas?

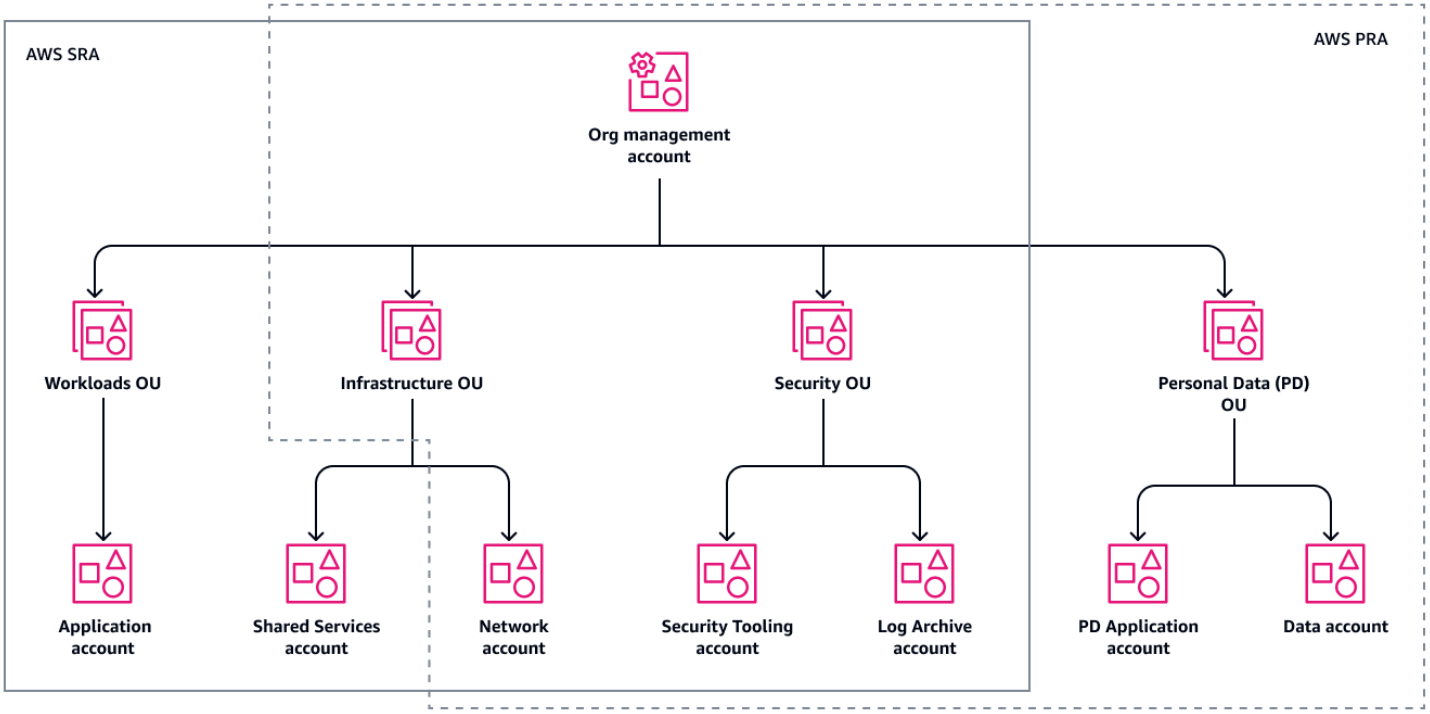
Las respuestas a muchas de estas preguntas pueden tener implicaciones en el diseño de su entorno de nube, por ejemplo, en la Cuenta de AWS estructura, las políticas de control de servicios y las funciones AWS Identity and Access Management (IAM).

AWS Organizations y la estructura de cuentas dedicada

> **Encuesta**
>
> Nos encantaría saber su opinión. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

AWS Organizations es un servicio de administración de cuentas que le permite administrar y gestionar varias Cuentas de AWS de forma centralizada. El uso de AWS Organizations es la base de un entorno de múltiples AWS cuentas bien diseñado. Para obtener más información, consulte Establishing your best practice AWS environment.

El siguiente diagrama muestra la estructura de cuentas y unidades organizativas (OU) de alto nivel de la PRA. AWS 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 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 revelación 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 AWS SRA.
- 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 UO de datos personales.

Puede utilizar AWS Control Tower para aplicar una gobernanza básica general y para la implementación automatizada de los controles de seguridad y privacidad en toda su organización. Si su organización AWS Control Tower no lo utiliza actualmente, puede implementar muchos de los controles de seguridad y privacidad incluidos AWS Control Tower, como las políticas y AWS Config reglas de control de servicios, en sus respectivos servicios.

Puede que le ayude valorar el procesamiento de los datos personales al planificar su estructura de cuentas y UO, incluida una estrategia de segmentación de cuentas. Es posible que deba tener en cuenta los tipos de datos que procesa en función de sus casos de uso específicos y de la legislación y normativas aplicables. Por ejemplo, los datos de los titulares de las tarjetas están protegidos por el Estándar de Seguridad de Datos del Sector de las Tarjetas de Pago (PCI DSS) y la información sobre la salud protegida puede estar sujeta a la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) de EE. UU. Tal vez quiera revisar qué entornos contienen datos personales y planificar su estrategia de segmentación basándose en gran medida en ello. Las estrategias de segmentación de cuentas típicas pueden incluir Cuentas de AWS específicas que se adapten al ciclo de vida del desarrollo del software (SDLC), como cuentas dedicadas al desarrollo, las pruebas 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.

Algunos AWS entornos con varias cuentas requieren cuentas de aplicaciones dedicadas por zona de destino para varias cuentas Región de AWS, o pueden requerirla. En este caso, necesita una segmentación adicional para cumplir con los requisitos exclusivos de soberanía de datos en relación con sus clientes y los organismos reguladores. Para obtener más información, consulte la sección Preparación de estrategias para la expansión global de esta guía.

Operacionalización AWS de los servicios de privacidad

> **Encuesta**
>
> Nos encantaría saber su opinión. 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, incluso los equipos de regulación, cumplimiento e ingeniería. Cuando su organización haya empezado a definir las personas y los componentes de políticas 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 la aplicación para los datos personales en su entorno. AWS

Independientemente del marco que utilicen los clientes para clasificar sus requisitos en materia de privacidad, los equipos de cumplimiento de normas de privacidad, ingeniería de privacidad y

aplicaciones suelen tener que colaborar 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 ayudarlo a definir controles organizativos y técnicos más prescriptivos.

Al definir los controles técnicos Servicios de AWS y las funciones, 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, el bloqueo del 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 según los recursos.

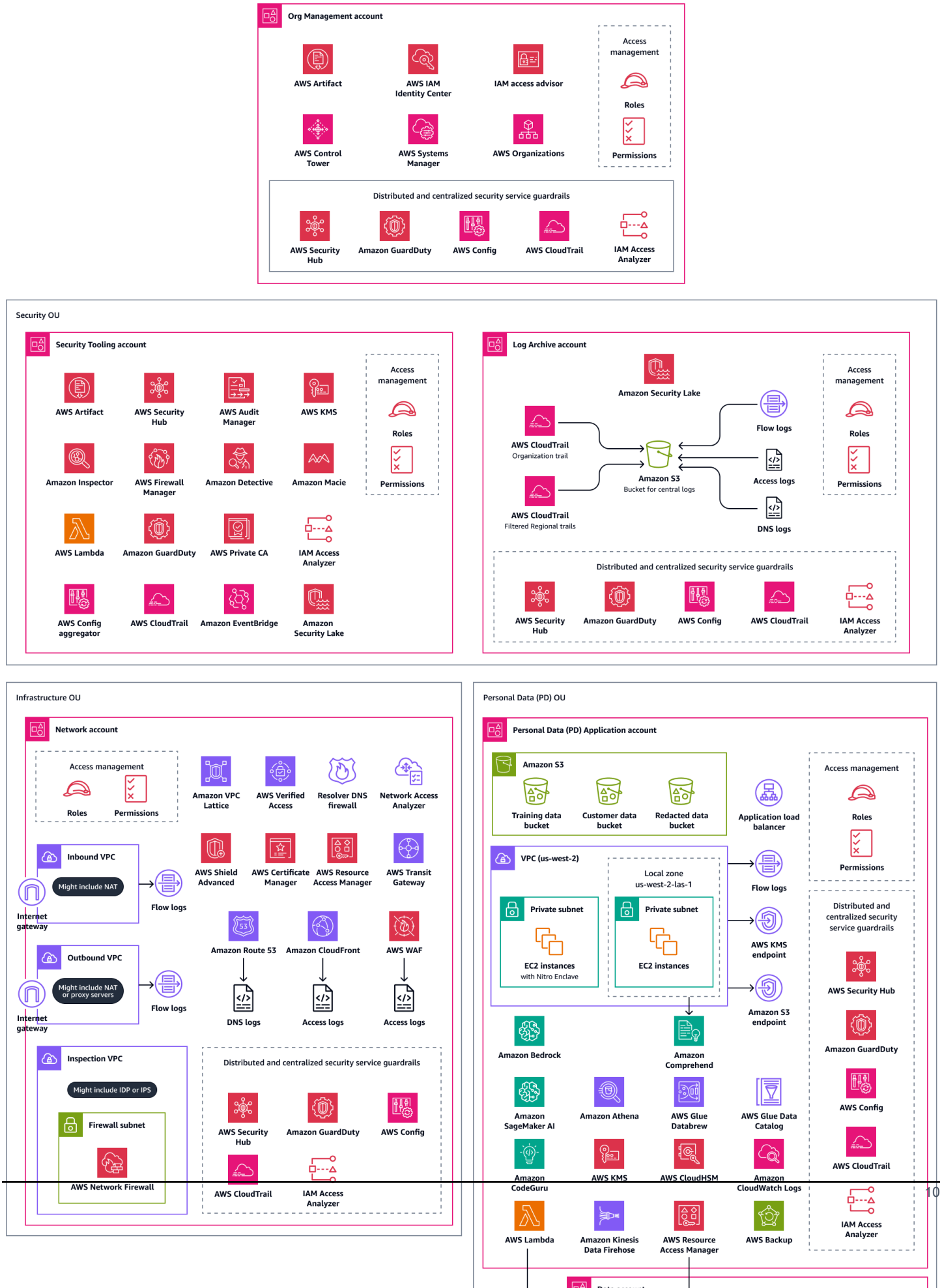
Para ayudarlo a acelerar la operacionalización de la privacidad en su organización, AWS ofrece servicios de asesoría de auditoría y cumplimiento para sus cargas de AWS trabajo. Para obtener más información, póngase en contacto con SAS AWS.

La arquitectura AWS de referencia de privacidad

Encuesta

Nos encantaría saber su opinión. 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 gobierna en AWS Control Tower.


Org Management account
AWS Artifact
AWS IAM Identity Center
IAM access advisor
Access management
Roles
Permissions
AWS Control Tower
AWS Systems Manager
AWS Organizations
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
Access management
Roles
Permissions
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
Amazon Security Lake
Log Archive account
Amazon Security Lake
AWS CloudTrail
Organization trail
Flow logs
Amazon S3
Bucket for central logs
Access logs
AWS CloudTrail
Filtered Regional trails
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
Amazon VPC Lattice
AWS Verified Access
Resolver DNS firewall
Network Access Analyzer
Inbound VPC
Might include NAT
Internet gateway
Flow logs
AWS Shield Advanced
AWS Certificate Manager
AWS Resource Access Manager
AWS Transit Gateway
Outbound VPC
Might include NAT or proxy servers
Internet gateway
Flow logs
Amazon Route 53
Amazon CloudFront
AWS WAF
DNS logs
Access logs
Access logs
Inspection VPC
Might include IDP 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
Personal Data (PD) OU
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
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
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 una 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).

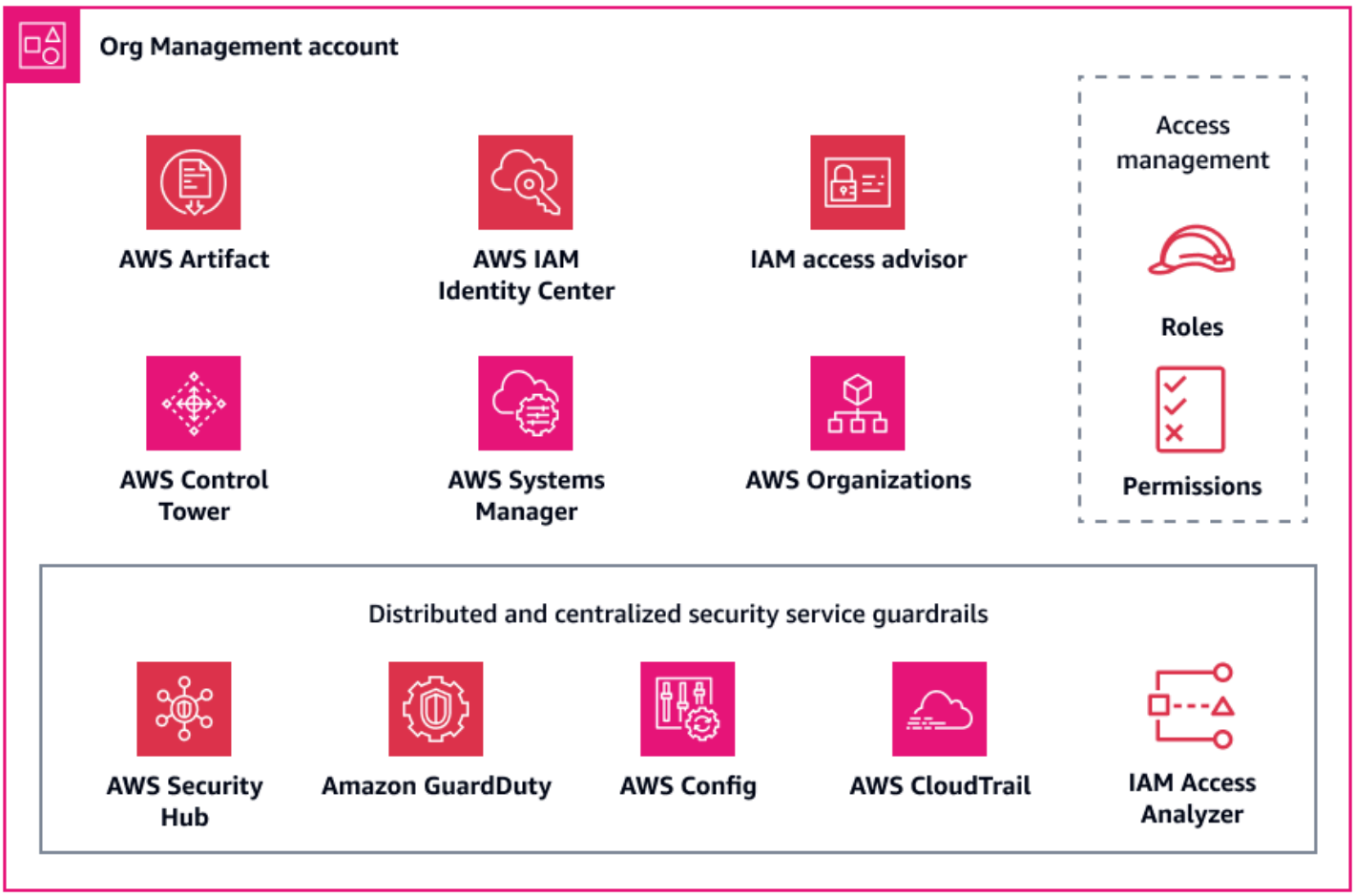
A continuación, en esta guía se describe en detalle cada cuenta de la organización. En ella se analizan los servicios y las características relacionados con la privacidad, las consideraciones y recomendaciones, y los diagramas correspondientes a cada una de las siguientes cuentas:

- Cuenta de administración de la organización
- UO de seguridad: cuenta de herramientas de seguridad
- UO de seguridad: cuenta de archivos de registro
- Unidad organizativa de infraestructura: cuenta de red
- UO de datos personales: cuenta de la aplicación de datos personales

Cuenta de administración de la organización

> **Encuesta**
>
> Nos encantaría saber su opinión. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

La cuenta de administración de la organización se usa principalmente para administrar la deriva de la configuración de los recursos para los controles de privacidad fundamentales en todas las cuentas de la organización, que está administrada 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 los siguientes Servicios de AWS que se utilizan en esta cuenta:

- AWS Artifact
- AWS Control Tower
- AWS Organizations

AWS Artifact

AWS Artifact puede ayudarlo con las auditorías al proporcionar descargas de documentos de seguridad y cumplimiento de AWS bajo demanda. Para obtener más información sobre cómo se utiliza este servicio en un contexto de seguridad, consulte la Arquitectura de referencia de seguridad de AWS.

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 y privacidad. Los siguientes informes pueden resultar útiles para demostrar la eficacia de los controles de privacidad de AWS :

- 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. También hay un informe de privacidad del SOC 3, que es una descripción menos detallada de los controles de privacidad del SOC 2. Para obtener más información, consulte las preguntas frecuentes sobre el SOC.
- Catálogo de controles de cumplimiento de la computación en la nube (C5): este informe fue creado por la autoridad nacional de ciberseguridad de Alemania, el Bundesamt für Sicherheit in der Informationstechnik (BSI). En él se detallan los controles de seguridad que implementó AWS para cumplir con los requisitos del C5. También incluye requisitos de control de la privacidad adicionales relacionados con la ubicación de los datos, el aprovisionamiento de servicios, el lugar de jurisdicción y las obligaciones de divulgación de información.
- Informe de certificación ISO/IEC 27701:2019: la ISO/IEC 27701:2019 describe los requisitos y directrices para establecer y mejorar continuamente un sistema de administración de la información de privacidad (PIMS). Este informe detalla el alcance de esta certificación y puede servir como prueba de AWS certificación. Para obtener más información sobre esta norma, consulte 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 prácticas recomendadas de seguridad prescriptivas. Para obtener más información sobre cómo se utiliza este servicio en un contexto de seguridad, consulte la Arquitectura de referencia de seguridad de AWS.

También puede automatizar el despliegue de muchos controles proactivos, preventivos y de detección, también conocidos como barreras de protección, que se ajustan a sus requisitos de privacidad de datos, específicamente en lo que respecta a la residencia y la soberanía de los datos. AWS Control Tower Por ejemplo, puede especificar barreras de protección que limiten la transferencia de datos únicamente a las Regiones de AWS aprobadas. 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 están compuestas por 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

En cuanto a la soberanía de los datos, AWS Control Tower actualmente proporciona controles preventivos, como Exigir que un volumen adjunto de Amazon EBS esté configurado para cifrar los datos en reposo y Requerir una política de AWS KMS claves para incluir una declaración que limite la creación de AWS KMS subvenciones a. Servicios de AWS Los controles de soberanía no son solo simples controles de residencia de datos. Ayudan a prevenir las acciones que podrían infringir los requisitos de residencia de datos, restricción de acceso detallado, cifrado y resiliencia. Para obtener más información, consulte Preventive controls that assist with digital sovereignty en la documentación de AWS Control Tower .

Si necesita implementar barreras de privacidad más allá de los controles de residencia y soberanía de los datos, AWS Control Tower incluye una serie de controles obligatorios. Estos controles se implementan de forma predeterminada en todas las UO al configurar la zona de aterrizaje. Muchos de estos son controles preventivos diseñados para proteger los registros, como impedir la eliminación del archivo de registros y habilitar la validación de la integridad del archivo de registro. CloudTrail

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

AWS Organizations

El AWS PRA se utiliza AWS Organizations para administrar de forma centralizada todas las cuentas dentro de la arquitectura. Para obtener más información, consulte la sección AWS Organizations y la estructura de cuentas 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 la organización, también puede implementar estos controles manualmente.

Se utiliza SCPs para abordar los requisitos de residencia de datos

Es habitual administrar los requisitos de residencia de datos personales almacenando y procesando los datos dentro de una región geográfica específica. Para verificar que se cumplan los requisitos de residencia de datos exclusivos de una jurisdicción, le recomendamos que colabore estrechamente con el equipo de regulación para confirmar los requisitos. Cuando se han 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 una política de ejemplo, consulte Restrinja las transferencias de datos entre Regiones de AWS en esta guía.

Se utiliza 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, usted es responsable de los resultados de las llamadas a la API que se puedan realizar en los Servicios de AWS que utiliza. También es responsable de comprender cuáles de esas llamadas podrían provocar cambios en su posición 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 infracción de determinadas transferencias de datos transfronterizas. Por ejemplo, tal vez quiera prohibir las siguientes llamadas a la API:

- Permitir el acceso público a buckets 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 DNSDataTrojan:EC2/ Exfiltration
- AWS WAF Eliminar las reglas de exfiltración de datos
- Compartir instantáneas de Amazon Elastic Block Store (Amazon EBS) públicamente
- 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 basado en atributos (ABAC) que limiten el acceso a los recursos que tengan una etiqueta o un conjunto de etiquetas específicos. Por ejemplo, la política podría especificar que el rol `SysAdmin` no puede acceder a los recursos que tengan 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 la organización usa AWS Backup para aplicar políticas de retención de datos de forma amplia en todas las copias de seguridad de muchas cuentas, puede aplicar una etiqueta que incluya ese recurso dentro del alcance de esa política de copias de seguridad.

Las políticas de etiquetas lo ayudan a mantener la coherencia de las etiquetas 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 casos válidos para las claves. También puede utilizar la aplicación para evitar que se completen las solicitudes de etiquetado que no cumplan los requisitos.

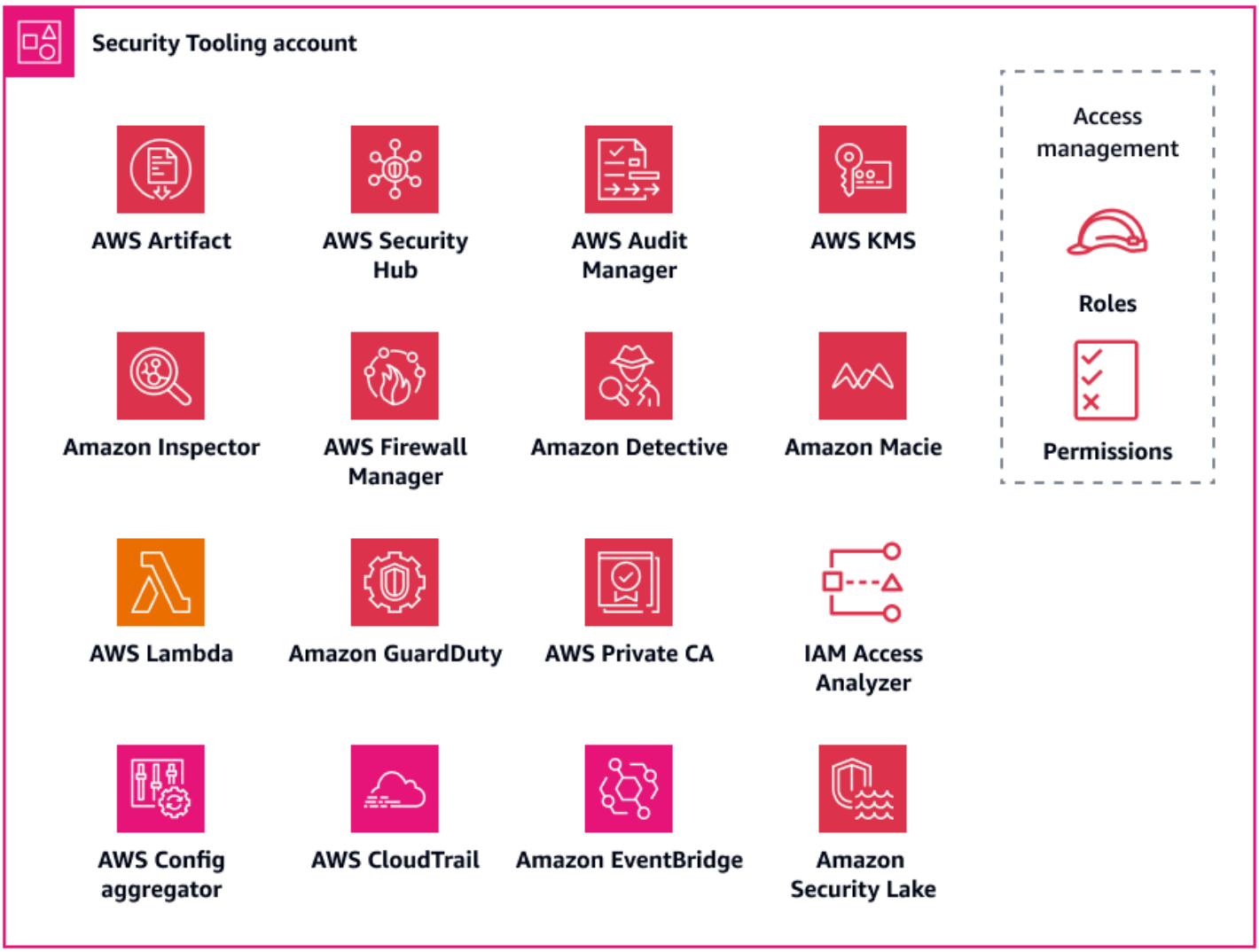
Cuando utilice las etiquetas como un componente fundamental de la estrategia de control de la privacidad, debe tener en cuenta lo siguiente:

- Tenga en cuenta las implicaciones de colocar datos personales u otros tipos de información confidencial dentro de las claves o los 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. Los datos de las etiquetas no están cifrados y Servicios de AWS, por ejemplo Administración de facturación y costos de AWS, pueden leerlos. Por lo tanto, es posible que desee desidentificar los valores de las etiquetas y, a continuación, volver a identificarlos mediante un sistema que usted controle, como un sistema de administración 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 dependen de las etiquetas.

UO de seguridad: cuenta de herramientas de seguridad

> **Encuesta**
>
> Nos encantaría saber su opinión. 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 los siguientes elementos de 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 de referencia de seguridad de AWS recomienda habilitar un rastro de la organización, que es un rastro único que registra todos los eventos de todas las cuentas de la organización. Sin embargo, al activar este rastro de la organización, se agregan los datos de registro de varias regiones en un único bucket de Amazon Simple Storage Service (Amazon S3) en la cuenta de archivos de registro. En el caso de las cuentas que gestionan datos personales, esto puede conllevar algunas consideraciones de diseño adicionales. Los registros pueden contener algunas referencias a datos personales. Para cumplir con los requisitos de residencia y transferencia de datos, es posible que deba volver a considerar la posibilidad de agregar los datos de registro entre regiones en una sola región en la que se encuentre el bucket de S3. La organización podría valorar qué cargas de trabajo regionales se deben incluir o excluir del rastro de la organización. En el caso de las cargas de trabajo que decida excluir del rastro de la organización, podría considerar la posibilidad de configurar un rastro específico para cada región que oculte los datos personales. Para obtener más información sobre el enmascaramiento de datos personal, consulte la sección Amazon Data Firehose de esta guía. En última instancia, la organización puede tener una combinación de rastros de la organización y rastros regionales que se agregan a la cuenta centralizada de archivos de registro.

Para obtener más información sobre cómo configurar un rastro de una sola región, consulta las instrucciones para usar la 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 administrar la centralización de los registros y los requisitos de transferencia de datos, consulte la sección Almacenamiento de registros centralizado de esta guía. Sea cual sea la configuración que elija, es posible que desee separar la administración de pistas en la cuenta de Security Tooling del almacenamiento de registros en la cuenta de Log Archive, según la AWS SRA. Este diseño lo ayuda a crear políticas de acceso con privilegios mínimos para quienes tengan que administrar los registros y quienes tengan que usar los datos de registro.

AWS Config

AWS Config proporciona una visión detallada de los recursos de su Cuenta de AWS y de cómo están configurados. Lo 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 de referencia de seguridad de AWS.

En AWS Config ella, 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 Prácticas operativas recomendadas para el NIST Privacy Framework v1.0 está alineado con una serie de controles relacionados con la privacidad del NIST Privacy Framework. Cada AWS Config regla se aplica a un tipo de AWS recurso específico y está relacionada con uno o más controles del marco de privacidad del NIST. Puede usar este paquete de conformidad para comprobar el cumplimiento continuo relacionado con la privacidad en todos los recursos de sus cuentas. A continuación, se describen 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 de salida `0.0.0.0/0` o `::/0` predeterminadas a una puerta de enlace de Internet. Esto lo 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 se han cifrado los volúmenes de Amazon Elastic Block Store (Amazon EBS) que están asociados a instancias de Amazon Elastic Compute Cloud (Amazon EC2). Si su organización tiene requisitos de control específicos relacionados con el uso de claves AWS Key Management Service (AWS KMS) para la protección de 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 seguridad de Amazon EC2 permiten el tráfico TCP sin restricciones a los puertos especificados. 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 `0.0.0.0/0` a los puertos comunes, como el TCP 3389 y el TCP 21, lo ayuda a restringir el acceso remoto.

AWS Config se pueden utilizar para realizar comprobaciones de conformidad proactivas y reactivas de sus recursos. AWS Además de tener en cuenta las reglas que se encuentran en los paquetes de conformidad, puede incorporarlas en los modos de evaluación de prevención 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 Amazon EC2 con 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 de seguridad de AWS.

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 avisarle 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 instancias de EC2 o llamadas inusuales de 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 puede considerar la posibilidad de identificar todas las partes interesadas relacionadas con la privacidad en el proceso de respuesta a incidentes, desde la detección y el análisis hasta la contención y la erradicación, e involucrarlas en cualquier incidente que podría implicar una 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 que se han aprobado y previsto previamente, y no con otras entidades. Un perímetro de datos es un conjunto de barreras de protección de prevención que se ha diseñado para permitir que solo las identidades de confianza procedentes de las redes esperadas accedan a los recursos de confianza de su entorno de AWS . Al definir los controles para evitar la divulgación intencionada o no intencionada de datos personales, puede definir las identidades de confianza, los recursos de confianza 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 las alertas en caso de infracciones en esa zona de confianza. El Analizador de acceso de IAM analiza las políticas de IAM para ayudar a identificar y resolver el acceso entre cuentas o público no intencionado a los recursos potencialmente confidenciales. El Analizador de acceso de IAM utiliza la lógica matemática y la inferencia para generar resultados exhaustivos sobre los recursos a los que se puede acceder desde fuera de una Cuenta de AWS. Por último, para responder a las políticas de IAM que sean demasiado permisivas y corregirlas, puede utilizar el Analizador de acceso de IAM para validar las políticas actuales al compararlas con las prácticas recomendadas de IAM y ofrecer sugerencias. El Analizador de acceso de IAM puede generar una política de IAM con privilegios mínimos que se base en la actividad de acceso previa de una entidad principal 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 el Analizador de acceso de IAM se utiliza este servicio en un contexto de seguridad, consulte la Arquitectura de referencia de seguridad de AWS.

Amazon Macie

Amazon Macie es un servicio que utiliza el machine learning y la coincidencia de patrones para detectar información confidencial, proporciona visibilidad de los riesgos de seguridad de los datos y permite automatizar las protecciones contra esos riesgos. Macie genera resultados cuando detecta posibles infracciones de políticas o problemas con la seguridad o la privacidad de los buckets de Amazon S3. Macie es otra herramienta que las organizaciones pueden usar para implementar la automatización y 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 de seguridad de AWS.

Macie puede detectar una amplia lista creciente de tipos de información confidencial, 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 según su organización.

A medida que su organización defina controles de prevención para los buckets de Amazon S3 que contienen datos personales, puede usar Macie como mecanismo de validación para saber con certeza en todo momento dónde se encuentran los datos personales y cómo están protegidos. Para empezar, active Macie y configure la detección automática de información confidencial. 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 en el que se muestra dónde se encuentran los datos personales. La característica de detección automática de información confidencial está diseñada para reducir los costos y minimizar la necesidad de configurar manualmente las tareas de detección. Puede aprovechar la característica de detección automática de información confidencial y utilizar Macie para detectar automáticamente los nuevos buckets o los nuevos datos en los buckets 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 buckets que se han clasificado incorrectamente o no se han clasificado.

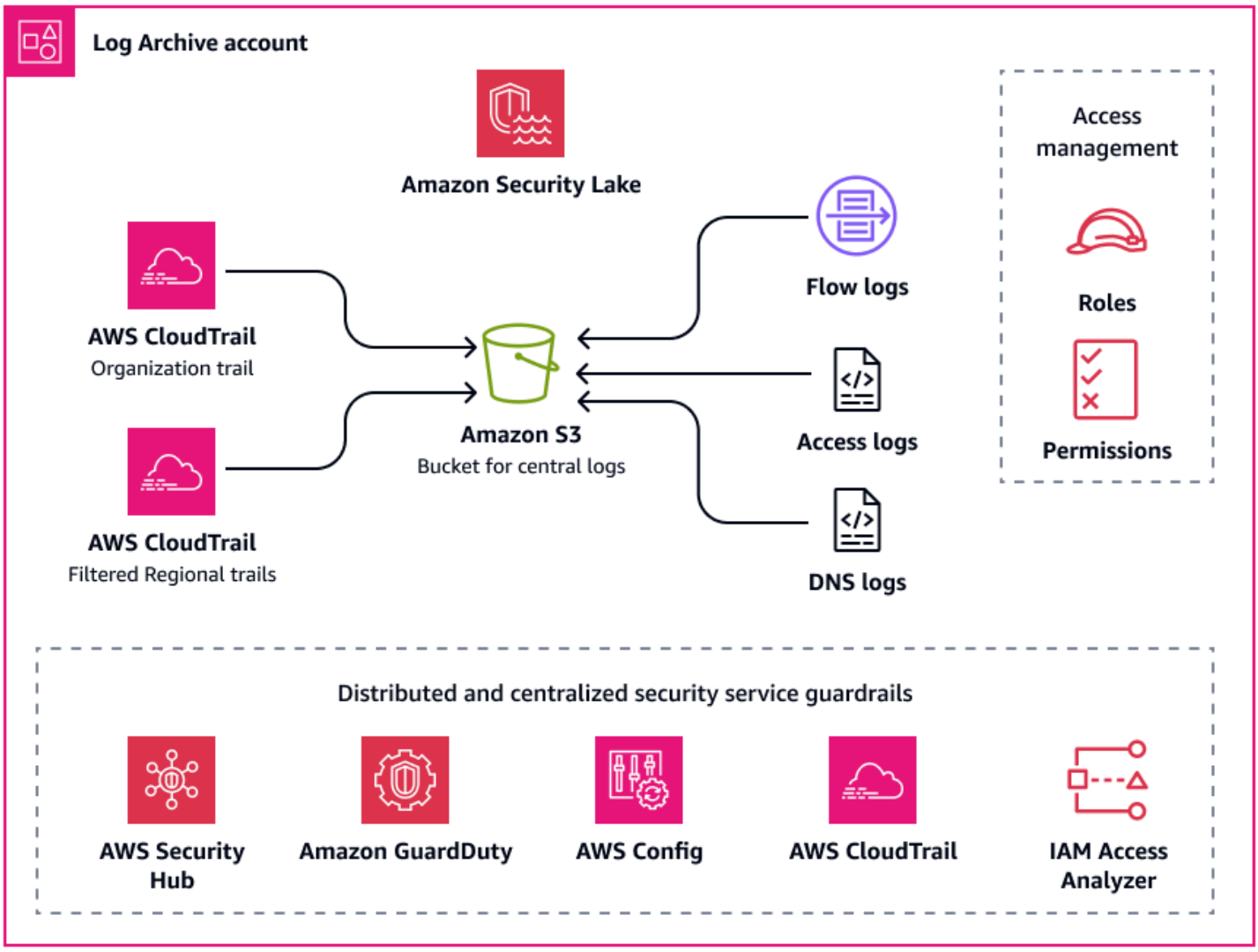
Puede habilitar Macie para todas las cuentas de su organización mediante. AWS Organizations Para obtener más información, consulte Integrating and configuring an organization in Amazon Macie.

UO de seguridad: cuenta de archivos de registro

> **Encuesta**
>
> Nos encantaría saber su opinión. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

La cuenta de archivos de registro 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 específica para los registros, puede aplicar alertas coherentes en todos los tipos de registros y confirmar que el personal de respuesta a incidentes pueda acceder a un conjunto de estos registros desde un solo lugar. También puede configurar los controles de seguridad y las políticas de retención de datos desde un solo lugar, lo que puede simplificar la sobrecarga operativa de privacidad. En el siguiente diagrama,

se ilustran los servicios de seguridad y privacidad de AWS que se pueden configurar en la cuenta de archivos de registro.



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.

Según la definición de datos personales de su organización, sus obligaciones contractuales en relación con los clientes y las normas de privacidad regionales aplicables, es posible que deba tener en cuenta las transferencias de datos transfronterizas en lo que respecta a la agregación de registros. Determine si los datos personales de los distintos tipos de registro están sujetos a estas restricciones. Por ejemplo, CloudTrail los registros pueden contener datos de los empleados de su organización, pero es posible que no contengan los datos personales de sus clientes. Si su organización tiene que cumplir con requisitos de transferencia de datos restringidos, las siguientes opciones pueden resultarle útiles:

- 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.
- Redacte los datos personales que deben permanecer en ella Región de AWS antes de copiarlos y agregarlos a otra región. Por ejemplo, puede enmascarar los datos personales de la región del host de la aplicación antes de transferir los registros a otra región. Para obtener más información sobre el enmascaramiento de datos personal, consulte la sección Amazon Data Firehose de esta guía.
- Si tienes problemas estrictos sobre la soberanía de los datos, puedes mantener una landing zone independiente para múltiples cuentas en la Región de AWS que se apliquen estos requisitos. De esta forma, puede simplificar la configuración de la zona de aterrizaje en la región para centralizar los registros. También proporciona otras ventajas de división de la infraestructura y ayuda a mantener el registro local en su propia región. Trabaje con su asesor legal para determinar qué datos personales están incluidos en el ámbito de aplicación y qué Region-to-Region transferencias están permitidas. Para obtener más información, consulte la sección Preparación de estrategias para la expansión global de esta guía.

A través de los registros de servicio, los registros de aplicaciones y los registros del sistema operativo (SO), puedes usar Amazon CloudWatch para monitorear Servicios de AWS los recursos de su cuenta y región correspondientes de forma predeterminada. Muchos optan por centralizar estos registros y métricas desde varias cuentas y regiones en una sola cuenta. De forma predeterminada, estos registros se conservan en la cuenta y la región correspondientes en las que se originan. Para la centralización, puede usar filtros de suscripción y tareas de exportación de Amazon S3 para

compartir los datos en una ubicación centralizada. Puede ser importante incluir los filtros y las tareas de exportación adecuados al agregar registros de una carga de trabajo que tenga requisitos para las transferencias de datos transfronterizas. Si los registros de acceso de una carga de trabajo contienen datos personales, es posible que tenga que asegurarse de que se transfieran a cuentas y regiones específicas o que se retengan en ellas.

Amazon Security Lake

Como se recomienda en la AWS SRA, es posible que desee utilizar la cuenta Log Archive como cuenta de administrador delegado para Amazon Security Lake. Si la utiliza para ello, Security Lake recopilará los registros compatibles en buckets de Amazon S3 específicos en la misma cuenta que otros registros de seguridad recomendados por SRA.

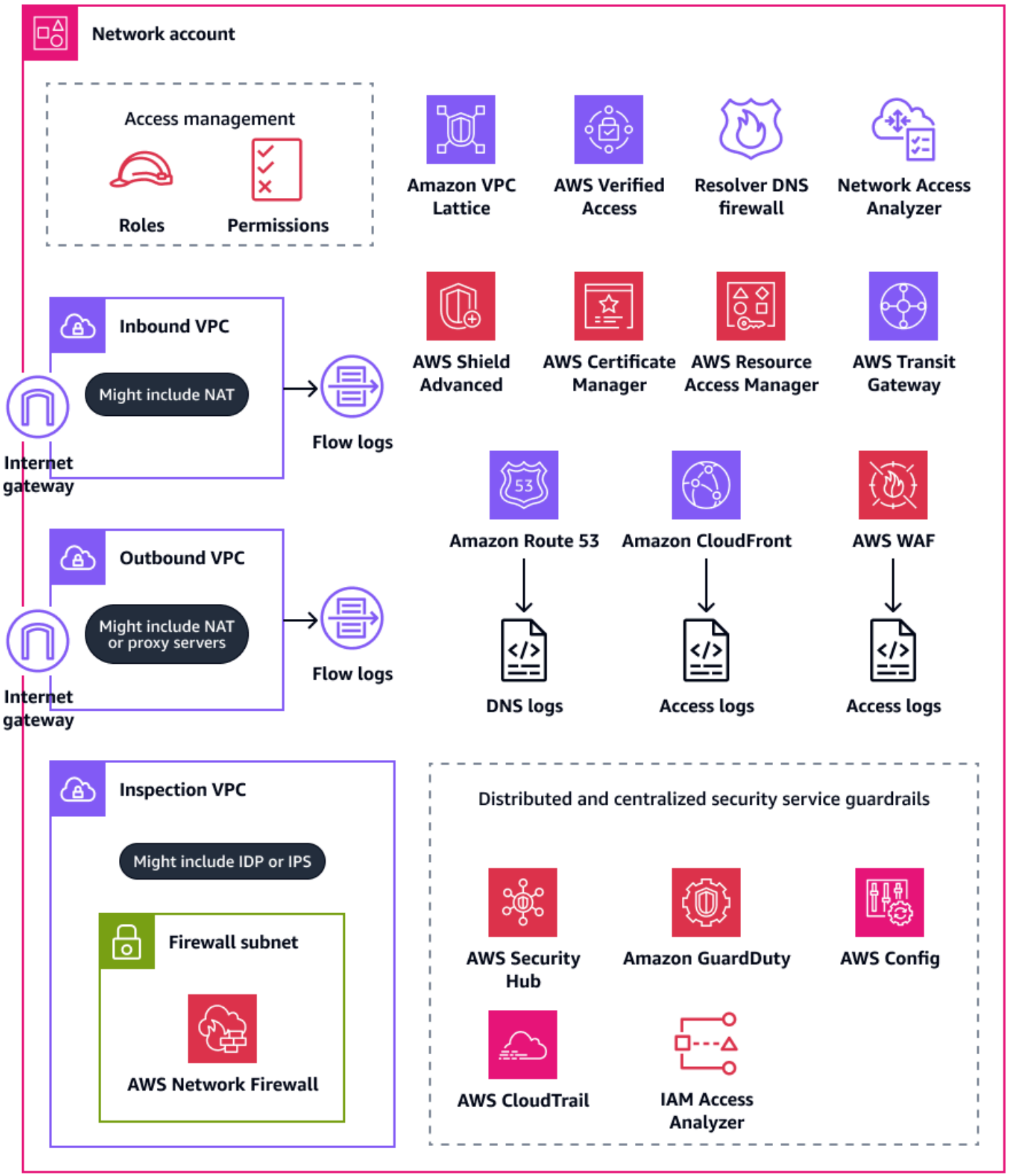
Desde el punto de vista de la privacidad, es importante que el personal de respuesta a incidentes tenga acceso a los registros de sus AWS entornos, proveedores de SaaS, locales, fuentes en la nube y fuentes de terceros. Esto los ayuda a bloquear y corregir más rápidamente el acceso no autorizado a los datos personales. Es muy probable que las mismas consideraciones para el almacenamiento de registros se apliquen a la residencia de registros y al movimiento entre regiones dentro de Amazon Security Lake. Esto se debe a que Security Lake recopila los registros y eventos de seguridad desde Regiones de AWS los que se ha activado el servicio. Para cumplir con los requisitos de residencia de datos, tenga en cuenta la configuración de las regiones acumulativas.Una región acumulativa es una región en la que Security Lake consolida los datos de una o más regiones contribuyentes que usted haya seleccionado. Es posible que la organización tenga que ajustar los requisitos de cumplimiento de las regiones en materia de residencia de datos antes de poder configurar Security Lake y las regiones acumulativas.

Unidad organizativa de infraestructura: cuenta de red

> **Encuesta**
>
> Nos encantaría saber su opinión. 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
Amazon VPC Lattice
AWS Verified Access
Resolver DNS firewall
Network Access Analyzer
AWS Shield Advanced
AWS Certificate Manager
AWS Resource Access Manager
AWS Transit Gateway
Inbound VPC
Might include NAT
Internet gateway
Flow logs
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 IDP 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 los siguientes Servicios de AWS que se utilizan 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 de seguridad de AWS.

Es posible que el programa de privacidad ya tenga en cuenta el cumplimiento de leyes regionales específicas. Si la carga de trabajo está destinada a prestar servicios únicamente a clientes que residen exclusivamente en estas regiones, podría implementar medidas técnicas que impidan el uso desde otras regiones. Puedes usar restricciones CloudFront geográficas para impedir que los usuarios de ubicaciones geográficas específicas accedan al contenido que estás 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. En el caso de algunas organizaciones, el almacenamiento en caché entre regiones podría estar sujeto a requisitos de transferencias de datos transfronterizas.

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 capacidad de auditoría.

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 compartes una conexión de plano de datos con otra Cuenta de AWS, podrías considerar la posibilidad de establecer procesos para comprobar que las conexiones se realizan según las aprobaciones previas Regiones de AWS y cumplen con tus requisitos de residencia de datos. AWS RAM

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 en la sección UO de datos personales: cuenta de la aplicación 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 datos de su organización y cuenta con las medidas técnicas adecuadas, considere la posibilidad de implementar barreras de protección para evitar flujos de datos transfronterizos no autorizados en los planos de control y datos. En el plano de control, puede limitar el uso de las regiones y, en consecuencia, los flujos de datos entre regiones mediante políticas de control de servicio y de IAM.

Tiene 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 una zona de AWS aterrizaje más amplia, puedes 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, en AWS Transit Gateway puede hacer lo siguiente:

- Confirma que las conexiones este-oeste y norte-sur entre tu entorno y el local cumplen tus requisitos de VPCs privacidad.
- Configurar los ajustes de VPC según las necesidades 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 una política de control de servicio de ejemplo, consulte Restricción de la realización de cambios en las configuraciones de VPC en esta 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 de referencia de seguridad de AWS.

Con AWS WAFél, puede definir e implementar reglas que inspeccionen 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 malintencionadas
- os 10 principales ataques del Open Worldwide Application Security Project (OWASP), incluidos los ataques relacionados con la exfiltración, como la inyección de código SQL
- Frecuencias de solicitudes elevadas
- 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 contiene reglas diseñadas para bloquear los patrones de solicitud asociados a la explotación de bases de datos SQL, como los ataques por inyección de código SQL. Considere este grupo de reglas si la aplicación interactúa con una base de datos SQL.
- Entradas incorrectas conocidas: este grupo contiene reglas diseñadas para bloquear los patrones de solicitud que se conocen por no ser válidos y que están asociados a la explotación o la detección de vulnerabilidades.
- Control de bots: este grupo contiene reglas diseñadas para administrar las solicitudes de los bots, que pueden consumir un exceso de recursos, distorsionar las métricas de la empresa, provocar tiempos de inactividad y realizar actividades malintencionadas.

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

UO de datos personales: cuenta de la aplicación de datos personales

> **Encuesta**
>
> Nos encantaría saber su opinión. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

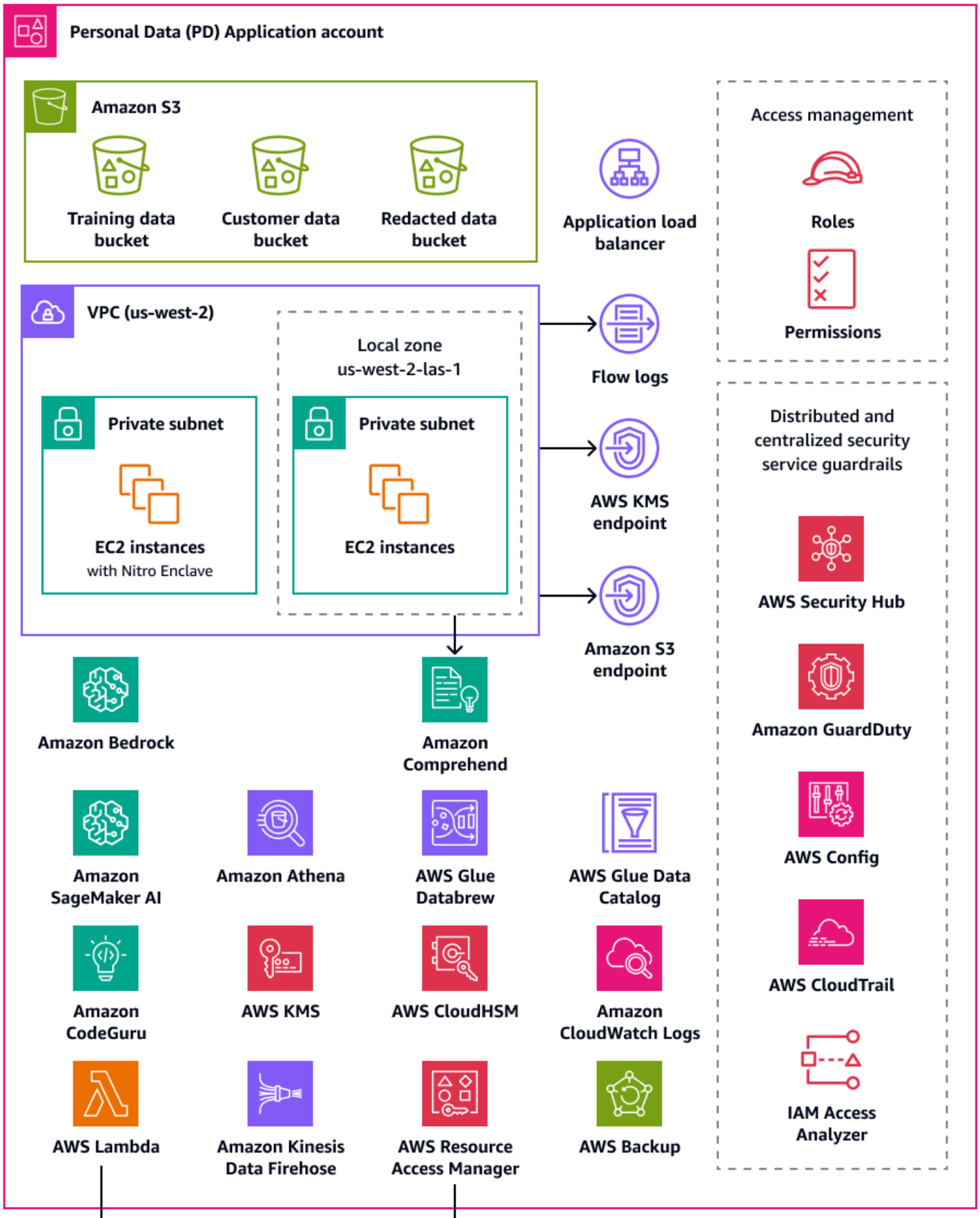
La cuenta de la aplicación de datos personales (PD) es el lugar donde la organización aloja los servicios que recopilan y procesan los datos personales. En concreto, en esta cuenta puede almacenar lo que defina como datos personales. La AWS PRA muestra varios ejemplos de configuraciones de privacidad 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 la 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 que establezca una unidad organizativa (UO) específica para estas cuentas. Por ejemplo, tal vez desee aplicar barreras de protección para la 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 podría considerar la posibilidad de crear una cuenta de datos dedicada, que es donde almacena el origen autorizado de sus conjuntos de datos personales. Los orígenes de datos autorizados son la ubicación donde se almacena la versión principal de los datos, que puede considerarse la versión más fiable y precisa de los datos. Por ejemplo, puede copiar los datos del origen de datos autorizado a otras ubicaciones, como los buckets de Amazon Simple Storage Service (Amazon S3) en la cuenta de la aplicación de datos personales que se utilizan para

almacenar datos de entrenamiento, un subconjunto de datos de clientes y datos con información suprimida. Al adoptar este enfoque de varias cuentas para separar los conjuntos de datos personales completos y definitivos que hay en la cuenta de datos de las cargas de trabajo de los consumidores posteriores que hay en la cuenta de la aplicación de datos personales, puede reducir el alcance del impacto en caso de acceso no autorizado a las 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
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Amazon Bedrock
Amazon Comprehend
Amazon SageMaker AI
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
Data account
Access management

En esta sección se proporciona información más detallada sobre los siguientes Servicios de AWS que se utilizan en estas cuentas:

- Amazon Athena
- Amazon Bedrock
- AWS Clean Rooms
- Amazon CloudWatch Logs
- CodeGuru Revisor de Amazon
- Amazon Comprehend
- Amazon Data Firehose
- Amazon DataZone
- AWS Glue
- AWS Key Management Service
- AWS Lake Formation
- Zonas locales de AWS
- AWS Enclaves Nitro
- AWS PrivateLink
- AWS Resource Access Manager
- Amazon SageMaker AI
- AWS funciones que ayudan a gestionar el ciclo de vida de los datos
- Servicios de AWS y funciones que ayudan a segmentar los datos
- Servicios de AWS y funciones que ayudan a descubrir, clasificar o catalogar datos

Amazon Athena

Puede considerar los controles de limitación de las consultas de datos para cumplir sus 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 que cargue los datos en Athena; funciona directamente con los datos almacenados en los buckets de S3.

Un caso de uso habitual 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

limpiarlos enmascarando columnas enteras de datos personales que proporcionen 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 para la transformación de datos necesita más flexibilidad de la que ofrecen 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 Bedrock

Amazon Bedrock es un servicio totalmente gestionado que proporciona acceso a los modelos básicos de las principales empresas de IA, como AI21 Labs, Anthropic, Meta, Mistral AI y Amazon. Ayuda a las organizaciones a crear y escalar aplicaciones de IA generativa. Independientemente de la plataforma que se utilice, al utilizar la IA generativa, las organizaciones podrían exponerse a riesgos de privacidad, como la posible exposición de los datos personales, el acceso no autorizado a los datos y otras infracciones relacionadas con el cumplimiento.

Las Barreras de protección para Amazon Bedrock están diseñadas para ayudar a mitigar estos riesgos mediante la aplicación de las prácticas recomendadas de seguridad y cumplimiento en todas sus cargas de trabajo de IA generativa en Amazon Bedrock. Es posible que la implementación y el uso de los recursos de IA no siempre se ajusten a los requisitos de privacidad y cumplimiento de una organización. Las organizaciones pueden tener dificultades para mantener la privacidad de los datos cuando utilizan modelos de IA generativa porque estos modelos pueden memorizar o reproducir información confidencial. Las Barreras de protección para Amazon Bedrock ayudan a proteger la privacidad, ya que evalúan las entradas de los usuarios y las respuestas de los modelos. En general, si los datos de entrada contienen datos personales, existe el riesgo de que esta información quede expuesta en la salida del modelo.

Las Barreras de protección para Amazon Bedrock proporcionan mecanismos para hacer cumplir las políticas de protección de datos y ayudan a evitar la exposición no autorizada de los datos. Ofrece funciones de filtrado de contenido para detectar y bloquear los datos personales en las entradas, restricciones temáticas para evitar el acceso a temas poco adecuados o peligrosos y filtros de palabras para enmascarar o suprimir términos delicados en las peticiones y respuestas de los modelos. Estas funciones ayudan a prevenir situaciones que podrían dar lugar a infracciones

de la privacidad, como las respuestas sesgadas o la erosión de la confianza de los clientes. Estas características pueden ayudarlo a garantizar que los modelos de IA no procesen ni revelen datos personales de forma accidental. Las Barreras de protección para Amazon Bedrock también admiten la evaluación de las entradas y las respuestas fuera de Amazon Bedrock. Para obtener más información, consulte Implement model-independent safety measures with Amazon Bedrock Guardrails (entrada en el blog de AWS).

Con las Barreras de protección para Amazon Bedrock, puede limitar el riesgo de alucinaciones de los modelos mediante comprobaciones de fundamento contextual, que evalúan la veracidad de los hechos y la relevancia de las respuestas. Un ejemplo es la implementación de una aplicación de IA generativa orientada al cliente que utiliza orígenes de datos externos en una aplicación de generación aumentada por recuperación (RAG). Las comprobaciones de fundamento contextual se pueden utilizar para validar las respuestas del modelo en comparación con estos orígenes de datos y filtrar las respuestas inexactas. En el contexto de la AWS PRA, puede implementar Amazon Bedrock Guardrails en todas las cuentas de carga de trabajo, donde aplica barreras de privacidad específicas que se adaptan a los requisitos de cada carga de trabajo.

AWS Clean Rooms

A medida que las organizaciones buscan formas de colaborar entre ellas mediante el análisis de conjuntos de datos confidenciales que se cruzan o se superponen, es crucial mantener la seguridad y la privacidad de esos datos compartidos. AWS Clean Rooms lo ayuda a implementar salas limpias de datos, que son entornos seguros y neutrales en los que las organizaciones pueden analizar conjuntos de datos combinados sin compartir los propios datos sin procesar. También puede generar información única al proporcionar acceso a otras organizaciones AWS sin mover ni copiar datos de sus propias cuentas y sin revelar el conjunto de datos subyacente. Todos los datos permanecen en la ubicación de origen. Las reglas de análisis integradas limitan la salida y restringen las consultas SQL. Todas las consultas se registran y los miembros de la colaboración pueden ver cómo se consultan los datos.

Puede crear una AWS Clean Rooms colaboración e invitar a otros AWS clientes a ser miembros de esa colaboración. A continuación, concede a un miembro la posibilidad de consultar los conjuntos de datos de los miembros y elige miembros adicionales para recibir los resultados de esas consultas. Si más de un miembro tiene que consultar los conjuntos de datos, puede crear colaboraciones adicionales con los mismos orígenes de datos y distintas configuraciones de miembros. Cada miembro puede filtrar los datos que se comparten con los miembros de la colaboración, y puede usar reglas de análisis personalizadas para establecer limitaciones sobre la forma en que se pueden analizar los datos que aportan a la colaboración.

Además de restringir los datos que se presentan a la colaboración y la forma en que otros miembros pueden utilizarlos, AWS Clean Rooms ofrece las siguientes funciones que pueden ayudarle a proteger la privacidad:

- La privacidad diferencial es una técnica matemática que mejora la privacidad del usuario al agregar a los datos una cantidad de ruido calibrada cuidadosamente. De esta forma, se reduce el riesgo de que se vuelva a identificar a los usuarios individuales en el conjunto de datos sin ocultar los valores de interés. El uso de la privacidad diferencial de AWS Clean Rooms no requiere ningún conocimiento experto en privacidad diferencial.
- AWS Clean Rooms ML permite que dos o más partes identifiquen a usuarios similares en sus datos sin compartir directamente sus datos entre sí. Esto reduce el riesgo de ataques de inferencia de miembros, en los que un miembro de la colaboración puede identificar a las personas del conjunto de datos del otro miembro. Al crear un modelo similar y generar un segmento similar, AWS Clean Rooms ML le ayuda a comparar conjuntos de datos sin exponer los datos originales. Esto no requiere que ninguno de los miembros tenga experiencia en aprendizaje automático ni que realice ningún trabajo ajeno a ellos. AWS Clean Rooms Usted mantiene el control total y la propiedad del modelo entrenado.
- Puede usar la computación criptográfica para Clean Rooms (C3R) con reglas de análisis para obtener información a partir de información confidencial. Limita criptográficamente lo que cualquier otra parte de la colaboración puede aprender. Al utilizar el cliente de cifrado C3R, los datos se cifran en el cliente antes de proporcionárselos. AWS Clean Rooms Como las tablas de datos se cifran con una herramienta de cifrado del cliente antes de cargarlas en Amazon S3, los datos permanecen cifrados y se conservan durante el procesamiento.

En la AWS PRA, le recomendamos que cree AWS Clean Rooms colaboraciones en la cuenta de datos. Puede utilizarlas para compartir los datos cifrados de los clientes con terceros. Úselas únicamente cuando haya una superposición en los conjuntos de datos proporcionados. Para obtener más información sobre cómo determinar la superposición, consulte la regla de análisis de listas en la AWS Clean Rooms documentación.

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 información confidencial, como datos personales, en los registros. La

política de protección de datos puede enmascarar esos datos cuando los usuarios acceden a los registros a través de la Consola de administración de AWS. Cuando los usuarios tengan que acceder directamente a los datos personales, de acuerdo con la especificación de finalidad general de la carga de trabajo, puede asignar permisos de `logs:Unmask` a esos usuarios. También tiene la opción de crear una política de protección de datos para toda la cuenta y aplicarla de forma coherente en todas las cuentas de la organización. Esto configura el enmascaramiento de forma predeterminada para todos los grupos de registros actuales y futuros en CloudWatch Logs. Además, recomendamos que active los informes de auditoría y los envíe a otro grupo de registro, 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 registro.

CodeGuru Revisor de Amazon

Tanto para la privacidad como para la seguridad, para muchas organizaciones es vital respaldar el cumplimiento constante durante la fase de implementación y las fases posteriores a la implementación. AWS PRA incluye controles proactivos en las canalizaciones 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 de seguridad, privacidad y recomendaciones generales. 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 código SQL
- Cookies sin protección
- Falta la autorización
- AWS KMS Recrificación del lado del cliente

Para obtener una lista completa de lo que CodeGuru Reviewer puede detectar, consulte la biblioteca de Amazon CodeGuru Detector.

Amazon Comprehend

Amazon Comprehend es un servicio de procesamiento de lenguaje natural (NLP) que usa machine learning para descubrir información y relaciones valiosas en documentos de texto en inglés. Amazon Comprehend puede detectar y suprimir datos personales en documentos de texto estructurados,

semiestructurados o sin estructurar. Para obtener más información, consulte Personally identifiable information (PII) en la documentación de Amazon Comprehend.

Dado que Amazon Comprehend ofrece muchas opciones para la integración de aplicaciones AWS SDKs, puede utilizar 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. En el diagrama de arquitectura de la cuenta de la aplicación de datos personales se muestra cómo puede realizar esta función para los registros de aplicaciones en Amazon EC2. Amazon Comprehend ofrece dos modos de supresión de datos:

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

Amazon Data Firehose

Puede usar Amazon Data Firehose para capturar, transformar y cargar datos de transmisión en directo en servicios posteriores, como Amazon Managed Service para Apache Flink o Amazon S3. Firehose se suele utilizar para transportar grandes cantidades de datos de transmisión en directo, como registros de aplicaciones, sin tener que crear 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 a las fases posteriores. Para conservar la privacidad, esta capacidad es compatible con 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 archivos de registro. Para obtener más información, consulte Biogen: solución de registro centralizada para cuentas múltiples (YouTube vídeo). En la cuenta de PD Application, configuras Amazon CloudWatch AWS CloudTrail para enviar los registros a una transmisión de entrega de Firehose. Una función de Lambda transforma los registros y los envía a un bucket de S3 central en la cuenta de archivos de registro. Puede configurar la función de Lambda para enmascarar campos específicos que contienen datos personales. Esto ayuda a evitar la transferencia de datos personales entre Regiones de AWS. Al utilizar este enfoque, los datos personales se enmascaran 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

transferencias transfronterizas, 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 AWS CloudTrail en la sección UO de seguridad: cuenta de herramientas de seguridad de esta guía.

Amazon DataZone

A medida que las organizaciones amplían su enfoque para compartir datos AWS Lake Formation, por Servicios de AWS ejemplo, quieren asegurarse de que el acceso diferencial esté controlado por quienes están más familiarizados con los datos: los propietarios de los datos. Sin embargo, es posible que estos propietarios de datos conozcan los requisitos de privacidad, como el consentimiento o las consideraciones sobre la transferencias de datos transfronterizas. Amazon DataZone ayuda a los propietarios de los datos y al equipo de gobierno de datos a compartir y consumir datos en toda la organización de acuerdo con sus políticas de gobierno de datos. En Amazon DataZone, las líneas de negocio (LOBs) administran sus propios datos y un catálogo rastrea esta propiedad. Las partes interesadas pueden buscar datos y solicitar acceso a ellos como parte de sus tareas comerciales. Siempre que cumpla con las políticas establecidas por los publicadores de datos, el propietario de los datos puede conceder el acceso a las tablas subyacentes sin necesidad de un administrador ni de mover los datos.

En un contexto de privacidad, Amazon DataZone puede ser útil en los siguientes casos de uso de ejemplo:

- Una aplicación orientada al cliente genera datos de uso que se pueden compartir con una línea de negocio de marketing independiente. Debe asegurarse de que solo se publiquen en el catálogo los datos de los clientes que hayan aceptado la opción de marketing.
- Los datos de los clientes europeos se publican, pero solo los usuarios LOBs locales del Espacio Económico Europeo (EEE) pueden suscribirlos. Para obtener más información, consulta Mejora la seguridad de los datos con controles de acceso detallados en Amazon. DataZone

En la AWS PRA, puede conectar los datos del bucket compartido de Amazon S3 a Amazon DataZone como productor de datos.

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 sin estructurar. 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 seguimiento de los datos atribuidos a un solo titular de los datos como parte de una solicitud del titular, la garantía de una calidad de datos uniforme y la segmentación general de los conjuntos de datos. AWS Glue es un servicio de extracción, transformación y carga (ETL) completamente administrado. 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 Catalog lo 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 almacén de datos. Ejecuta un rastreador de AWS Glue para hacer un inventario de los datos en una variedad de tipos de almacenes de datos. Agrega clasificadores integrados y personalizados al rastreador. 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 la organización utiliza AWS Lake Formation para administrar y proporcionar acceso con permisos detallados a bases de datos, tablas, filas y celdas, el Catálogo de datos es un componente clave. El catálogo de datos permite el intercambio de datos entre cuentas y le ayuda a utilizar el control de acceso basado en etiquetas para administrar su lago de datos a escala (AWS entrada del blog). Para obtener más información, consulte AWS Lake Formation en esta sección.

AWS Glue DataBrew

AWS Glue DataBrew lo 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 información confidencial en las canalizaciones de datos. También puede crear un mapa visual del linaje de los datos para comprender los distintos orígenes 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 mejor la procedencia de los datos personales y hacer un seguimiento de ellos. DataBrew le ayuda a ocultar los datos personales durante la preparación de los datos. Puede detectar datos personales como parte de un trabajo 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 uso de algoritmos hash, 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 las fases posteriores para realizar tareas de análisis, elaboración de informes y machine learning. Algunas de las técnicas de enmascaramiento de datos disponibles en DataBrew incluyen:

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

Estas son las técnicas de cifrado que hay 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 recomendar normas de calidad para su corrección. AWS Glue Data Quality también permite 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 seguridad de AWS.

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

- Usar claves administradas por el cliente para tener un mayor control sobre la resistencia, la rotación, la caducidad y otras opciones.
- Usar claves administradas por el cliente exclusivas 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 administrada por el cliente exclusiva para cada nivel. Por ejemplo, puede tener una clave para cifrar los datos operativos y otra para cifrar los datos personales.
- Impedir el acceso entre cuentas involuntario a claves de KMS.
- Almacenar las claves de KMS en el Cuenta de AWS mismo lugar 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 claves mediante barreras de protección de prevención y reacción.

De forma predeterminada, las claves de KMS se almacenan y solo se pueden utilizar en la región donde se crearon. Si la organización tiene requisitos específicos de soberanía y residencia de datos, considere si las claves de KMS de varias regiones son apropiadas para su caso de uso. Las claves

multirregionales son claves de KMS con un propósito especial y diferentes Regiones de AWS que se pueden usar indistintamente. El proceso de creación de una clave multirregional traslada el material clave más allá de Región de AWS las fronteras internas AWS KMS, por lo que esta falta de aislamiento regional podría no ser compatible con los objetivos de soberanía y residencia de la organización. Una forma de solucionar este problema consiste en utilizar un tipo diferente de clave de KMS, como una clave administrada por el cliente específica de una región.

Almacenes de claves externos

Para muchas organizaciones, el almacén de AWS KMS claves predeterminado Nube de AWS puede cumplir con sus requisitos de soberanía de datos y reglamentarios generales. Sin embargo, algunas organizaciones pueden necesitar que las claves de cifrado se creen y mantengan fuera de un entorno en la nube y que disponga de rutas de autorización y auditoría independientes. Con los almacenes de claves externos AWS KMS, puede cifrar los datos personales con material clave que su organización posea y controle de forma externa. Nube de AWS Seguirá interactuando con la AWS KMS API como de costumbre, pero solo AWS KMS interactúa con el software de proxy de almacén de claves externo (proxy XKS) que usted proporcione. A continuación, el proxy del almacén de claves externo interviene en todas las comunicaciones entre AWS KMS y el administrador de claves externo.

Al utilizar un almacén de claves externo para el cifrado de datos, es importante tener en cuenta el costo operativo adicional en comparación con el mantenimiento de las claves en AWS KMS. Con un almacén de claves externo, debe crear, configurar y mantener el almacén de claves externo. Además, si hay errores en la infraestructura adicional que debe mantener, como el proxy XKS, y se pierde la conectividad, es posible que los usuarios no puedan descifrar los datos ni acceder a ellos temporalmente. Debe trabajar en estrecha colaboración con las partes interesadas en materia de cumplimiento y normativas para comprender las obligaciones legales y contractuales relativas al cifrado de datos personales y sus acuerdos de nivel de servicio en relación con la disponibilidad y la resiliencia.

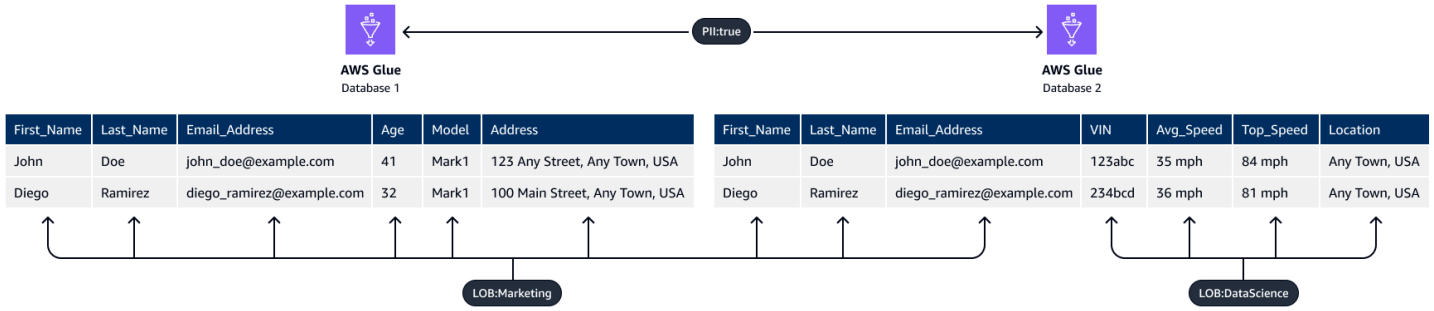
AWS Lake Formation

Muchas organizaciones que catalogan y categorizan sus conjuntos de datos mediante catálogos de metadatos estructurados desean compartir esos conjuntos de datos en toda la organización. Puede usar políticas de permisos AWS Identity and Access Management (IAM) para controlar el acceso a conjuntos de datos completos, pero a menudo se requiere un control más detallado para los conjuntos de datos que contienen datos personales de diferente sensibilidad. Por ejemplo, la especificación de la finalidad y la limitación de uso (sitio web de FPC) pueden indicar que un equipo

de marketing tiene que acceder a las direcciones de los clientes, pero un equipo de ciencia de datos no.

Los lagos de datos también suponen problemas de privacidad, ya que centralizan el acceso a grandes cantidades de información confidencial en su formato original. Se puede acceder de forma centralizada a la mayoría de los datos de una organización desde un solo lugar, por lo que la separación lógica de los conjuntos de datos, especialmente los que contienen datos personales, puede ser fundamental. AWS Lake Formation puede ayudarlo a configurar la gobernanza y la supervisión para compartir los datos, ya sea de un solo origen o de varios contenidos en un lago de datos. En la AWS PRA, puede usar Lake Formation para proporcionar un control de acceso detallado a los datos del depósito de datos compartido de la cuenta de datos.

Puede utilizar la característica de control de acceso basado en etiquetas en Lake Formation. El control de acceso basado en etiquetas es una estrategia de autorización que define permisos basados en atributos. En Lake Formation, estos atributos se denominan etiquetas LF. Con una etiqueta LF, puede adjuntar estas etiquetas a las bases de datos, tablas y columnas del Catálogo de datos y conceder las mismas etiquetas a las entidades principales de IAM. Lake Formation permite realizar operaciones en esos recursos cuando se concede acceso a la entidad principal a un valor de etiqueta que coincide con el valor de la etiqueta del recurso. En la siguiente imagen se muestra cómo asignar etiquetas LF y permisos para proporcionar un acceso diferenciado a los datos personales.



En este ejemplo, se usa la naturaleza jerárquica de las etiquetas. Ambas bases de datos contienen información de identificación personal (`PII:true`), pero las etiquetas en el nivel de columnas limitan las columnas específicas a los diferentes equipos. En este ejemplo, los directores de IAM que tienen la etiqueta `PII:true` LF pueden acceder a los recursos de la base de datos que tienen esta etiqueta. AWS Glue Las entidades principales con la etiqueta LF `LOB:DataScience` pueden acceder a columnas específicas que tengan esta etiqueta, y las entidades principales con la etiqueta LF `LOB:Marketing` solo pueden acceder a las columnas que tengan esta etiqueta. El equipo de marketing solo puede acceder a la PII que sea pertinente para los casos de uso de marketing y el equipo de ciencia de datos solo puede acceder a la PII que sea pertinente para sus casos de uso.

Zonas locales de AWS

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 utilizarlos Zonas locales de AWS, lo que le ayuda a ubicar los 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 en la cercanía geográfica 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 las zonas locales, tenga en cuenta los controles de residencia de datos que se hayan implementado en la organización. Por ejemplo, es posible que necesite un control para evitar las transferencias 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 al Zonas locales de AWS usar controles de landing zone (entrada del AWS blog).

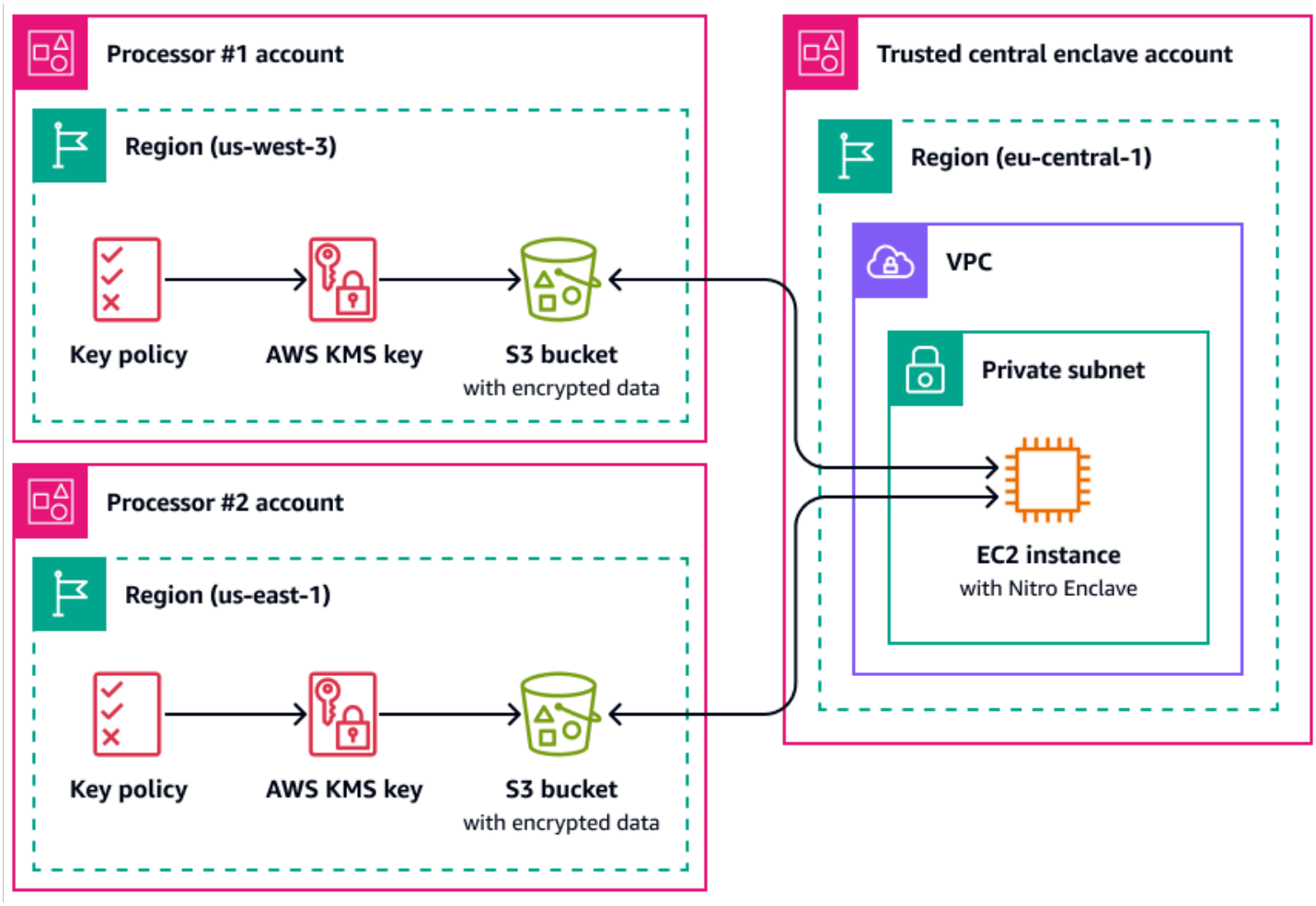
AWS Enclaves Nitro

Evalúe su estrategia de segmentación de datos desde el punto de vista del procesamiento, como el procesamiento de los datos personales con un servicio de computación 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 fiable. Los enclaves son máquinas virtuales independientes, reforzadas y muy restringidas. AWS Nitro Enclaves es una característica de Amazon EC2 que puede ayudarlo a crear estos entornos de computación aislados. Para obtener más información, consulte El diseño de seguridad del sistema AWS Nitro (documento técnico).AWS

Nitro Enclaves implementa un kernel que está separado del kernel de la instancia principal. El kernel de la instancia principal no tiene acceso al enclave. Los usuarios no pueden acceder a los datos y las aplicaciones del enclave mediante SSH ni de forma remota. Las aplicaciones que procesan datos personales pueden incrustarse en el enclave y configurarse para usar el socket Vsock del enclave, que permite que el enclave y la instancia principal se comuniquen.

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. En la siguiente imagen se muestra cómo se puede utilizar un enclave para el procesamiento

centralizado, una clave de KMS para cifrar los datos personales antes de enviarlos al enclave y una política de AWS KMS key que compruebe que el enclave que solicita el descifrado tenga las medidas únicas en el documento de certificación. Para obtener más información e instrucciones, consulte Uso de la atestación criptográfica con. AWS KMS Para ver una política de claves de ejemplo, consulte Exija una certificación para usar una clave AWS KMS en esta guía.



Con esta implementación, solo los procesadores de datos correspondientes 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 correspondientes procesadores de datos, es en el propio enclave, que está diseñado para evitar el acceso y las manipulaciones.

AWS PrivateLink

Muchas organizaciones quieren limitar la exposición de los datos personales a redes que no sean de confianza. Por ejemplo, si desea mejorar la privacidad del diseño general de la arquitectura de su 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 describe en la Servicios de

AWS y funciones 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 PrivateLink, puede configurar conexiones privadas específicas para los servicios que almacenan o procesan datos personales en su entorno; no es necesario que se conecte a los puntos de conexión públicos ni que transfiera 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 en el ámbito de aplicación, no se necesita una pasarela de Internet, un dispositivo NAT, una dirección IP pública, una conexión o una AWS Direct Connect conexión para poder 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 Obligación de 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. Puede compartir esos datos personales con otras cuentas de confianza a fin de poderlos procesar. 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 el intercambio si la cuenta del consumidor no forma parte de la organización

- Visibilidad de las entidades principales de IAM específicas que tienen acceso a cada recurso específico

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

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 para luego 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 SageMaker modelos Amazon

Muchas organizaciones tienen en cuenta la deriva de datos a la hora de entrenar modelos de ML. Una deriva de datos es una variación significativa entre los datos de producción y los datos que se utilizaron para entrenar un modelo de ML, o un cambio significativo en los datos de entrada a lo largo del tiempo. La deriva de 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 ML mientras está en producción se desvía de la naturaleza de los datos de referencia con los que se entrenó, la precisión de las predicciones podría disminuir. Amazon SageMaker 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 deriva de datos puede ayudarlo a implementar medidas correctivas, como el nuevo entrenamiento de modelos, la auditoría de los sistemas de las fases previas o la corrección de problemas de calidad de datos. El Monitor de modelos puede reducir la necesidad de supervisar manualmente los modelos o crear más herramientas.

Amazon SageMaker Clarify

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

las medidas del posible sesgo para que pueda 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 hay sesgos en los modelos ya entrenados revisando sus predicciones y supervisándolos continuamente para detectar sesgos. Por último, SageMaker 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 ayudarlo a determinar si la entrada de un modelo en particular 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. Entre estos detalles se pueden incluir el propietario del modelo, la finalidad general, los casos de uso previstos, las suposiciones realizadas, la clasificación de riesgo de un modelo, los detalles y las métricas del entrenamiento y los resultados de la evaluación. Para obtener más información, consulte Model Explainability with AWS Artificial Intelligence and Machine Learning Solutions (documentoAWS técnico).

Amazon SageMaker Data Wrangler

Amazon SageMaker Data Wrangler es una herramienta de aprendizaje automático que ayuda a agilizar el proceso de preparación de datos e ingeniería de características. Proporciona una interfaz visual que ayuda a los científicos de datos y a los ingenieros de machine learning a preparar y transformar los datos de forma rápida y sencilla para utilizarlos en modelos de machine learning. Con Data Wrangler, puede importar datos desde diversos orígenes, como Amazon S3, Amazon Redshift y Amazon Athena. A continuación, puede usar más de 300 transformaciones de datos integradas para limpiar, normalizar y combinar características sin tener que escribir ningún código.

Data Wrangler se puede utilizar como parte del proceso de preparación de datos e ingeniería de características en la PRA. AWS Admite el cifrado de datos en reposo y en tránsito mediante el uso AWS KMS, y utiliza las funciones y políticas de IAM para controlar el acceso a los datos y los recursos. Admite el enmascaramiento de datos a través de AWS Glue Amazon SageMaker Feature Store. Si integras Data Wrangler con AWS Lake Formation, puedes aplicar controles y permisos de acceso a los datos detallados. Incluso puede usar Data Wrangler con Amazon Comprehend

para suprimir automáticamente los datos personales de los datos tabulares como parte del flujo de trabajo más amplio de las operaciones de machine learning (MLOps). Para obtener más información, consulte Redactar automáticamente la PII para el aprendizaje automático mediante Amazon SageMaker Data Wrangler (AWS entrada del blog).

La versatilidad de Data Wrangler le permite enmascarar la información confidencial de muchos sectores, como números de cuentas, números de tarjetas de crédito, números de la seguridad social, nombres de pacientes e historiales médicos y militares. Puede limitar el acceso a cualquier información confidencial o elegir suprimirla.

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, debe considerar 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: un conjunto de reglas que definen acciones que Amazon S3 aplica a un grupo de objetos. En la configuración de Amazon S3 Lifecyle, 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, la retención y la eliminación de las instantáneas de Amazon Elastic Block Store (Amazon EBS) y de las Amazon Machine Images respaldadas por EBS (). AMIs
- Tiempo de duración (TTL) de DynamoDB: defina una marca temporal por elemento que determine cuándo ya no se necesita un elemento. Poco después de la fecha y hora de la marca temporal especificada, DynamoDB elimina el elemento de la tabla.

- Configuración de retención de CloudWatch registros en Logs: 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 sobre la actividad de copia de seguridad y cree informes la actividad desde una consola centralizada para cumplir con los requisitos de cumplimiento de las normas de copia de seguridad.

Servicios de AWS y funciones 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 ayudarlo 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 gran base de datos, puede segmentar estos datos en grupos más pequeños que sean más fáciles de administrar.

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

- Separación física: acción de almacenar los datos en almacenes de datos separados o de distribuirlos en recursos de AWS separados. Si bien los datos están separados físicamente, es posible que las mismas entidades principales puedan acceder a ambos recursos. Por eso le recomendamos que combine la separación física y la separación lógica.
- Separación lógica: acción de aislar los datos mediante controles de acceso. Los diferentes puestos laborales requieren diferentes niveles de acceso a subconjuntos de datos personales. Para ver un ejemplo de política que implementa la separación lógica, consulte Concesión de acceso a atributos específicos de Amazon DynamoDB en esta guía.

La combinación de una separación lógica y física brinda flexibilidad, simplicidad y detalle a la hora de redactar políticas basadas en la identidad y en los recursos para respaldar el acceso diferenciado entre los diferentes puestos laborales. Por ejemplo, desde el punto de vista operativo, crear políticas que separen de forma lógica las diferentes clasificaciones de datos en un único bucket de S3 puede ser complejo. El uso de buckets de S3 específicos para cada clasificación de datos simplifica la configuración y la administración de las políticas.

Servicios de AWS y funciones que ayudan a descubrir, clasificar o catalogar datos

Algunas organizaciones no han empezado a usar herramientas de extracción, carga y transformación (ELT) en su entorno para catalogar los datos de forma proactiva. Es posible que estos clientes se encuentren en una fase temprana de descubrimiento de datos, en la que deseen comprender mejor los datos que almacenan y procesan AWS y cómo están estructurados y clasificados. Puede utilizar Amazon Macie para comprender mejor los datos de PII en Amazon S3. Sin embargo, Amazon Macie no puede ayudarlo a analizar otros orígenes de datos, como Amazon Relational Database Service (Amazon RDS) y Amazon Redshift. Puede usar dos enfoques para acelerar la detección inicial al comienzo de un ejercicio de asignación de datos más amplio:

- Método manual: cree una tabla que tenga dos columnas y tantas filas como necesite. En la primera columna, escriba una caracterización de los datos (como nombre de usuario, dirección o género) que pueda aparecer en el encabezado o el cuerpo de un paquete de red o en cualquier servicio que proporcione. Pida al equipo de cumplimiento que complete la segunda columna. En la segunda columna, escriba “sí” si los datos se consideran personales y “no” si no lo son. Indique cualquier tipo de datos personales que se consideren especialmente confidenciales, como la denominación religiosa o los datos sobre la salud.
- Enfoque automatizado: utilice las herramientas que se proporcionan mediante AWS Marketplace. Una de esas herramientas es Securiti. Estas soluciones ofrecen integraciones con las que pueden escanear y detectar datos en varios tipos de recursos de AWS , así como activos en otras plataformas de servicios en la nube. Muchas de estas mismas soluciones pueden recopilar y mantener de forma continua un inventario de activos de datos y actividades de procesamiento de datos en un catálogo de datos centralizado. Si confía en una herramienta para realizar una clasificación automatizada, es posible que tenga que ajustar las reglas de detección y clasificación para adaptarlas a la definición de datos personales de la organización.

Ejemplos de políticas relacionadas con la privacidad

> **Encuesta**
>
> Nos encantaría saber su opinión. Envíe sus comentarios sobre la AWS PRA mediante una breve encuesta.

Muchas organizaciones que gestionan información confidencial adoptan un enfoque preventivo, con niveles de controles de detección y reacción implementados en todas las fases. Esta sección proporciona ejemplos de políticas relacionadas con la privacidad para AWS Identity and Access Management (IAM) AWS Organizations, y (). AWS Key Management Service AWS KMS Estas políticas pueden ayudar a su organización a cumplir distintos objetivos de privacidad relacionados con el uso, la limitación de la divulgación y las transferencias de datos transfronterizas mediante un enfoque preventivo. Muchas de estas políticas se mencionan en las secciones anteriores de esta guía.

En esta sección se incluyen las políticas de ejemplo siguientes:

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

Obligación del acceso desde direcciones IP específicas

> **Encuesta**
>
> Nos encantaría saber su opinión. Proporcione sus comentarios sobre la AWS PRA mediante una breve encuesta.

Esta política permite que el usuario `john_stiles` solo asuma roles de IAM si la llamada proviene de una dirección IP dentro de los intervalos `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 ubicadas en un subconjunto de áreas específicas Regiones de AWS. Además, debe comprobar la definición de PII de su organización, ya que algunas políticas pueden requerir secciones `Condition` o `Principal` que restrinjan el acceso a un usuario o dirección IP específicos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Effect": "Deny",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/john_stiles"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": [
            "192.0.2.0/24",
            "203.0.113.0/24"
          ]
        }
      }
    }
  ]
}
```

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

> **Encuesta**
>
> Nos encantaría saber su opinión. Proporcione 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 de prevención ayuda a establecer una zona de confianza y a definir el perímetro de 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 en 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

> **Encuesta**
>
> Nos encantaría saber su opinión. 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 usa un `NotAction` parámetro porque tiene en cuenta los servicios globales Servicios de AWS, como IAM, y los 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 como excepciones esos servicios globales y otros servicios no aplicables. Para obtener más información sobre cómo esta política puede ayudar a proteger la privacidad y los datos personales en su organización, consulte AWS Organizations en esta guía.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyAllOutsideEU",
            "Effect": "Deny",
            "NotAction": [
                "a4b:*",
                "acm:*",
                "aws-marketplace-management:*",
                "aws-marketplace:*",
                "aws-portal:*",
                "budgets:*",
                "ce:*",
                "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"
                    ]
                }
            }
```

```
        }
    ]
}
```

Concesión de acceso a atributos específicos de Amazon DynamoDB

> **Encuesta**
>
> Nos encantaría saber su opinión. 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 únicamente permite recuperar los atributos `UserID`, `SignUpTime` y `LastLoggedIn` de una tabla de Amazon DynamoDB llamada `Users`. Por ejemplo, puede asociar esta política a un rol de atención al cliente en lugar de darle acceso a este rol a todo el conjunto de datos personales. Para obtener más información sobre cómo esta política puede ayudar a proteger la privacidad y los datos personales en su organización, consulte Servicios de AWS y funciones que ayudan a segmentar los datos en esta guía.

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "dynamodb:GetItem",
            "dynamodb:BatchGetItem",
            "dynamodb:Query",
            "dynamodb:Scan"
         ],
         "Resource":[
            "arn:aws:dynamodb:us-west-2:123456789012:dynamodb:table/Users"
         ],
         "Condition":{
            "ForAllValues:StringEquals":{
```

```
                "dynamodb:Attributes":[
                   "UserID",
                   "SignUpTime",
                   "LastLoggedIn"
                ]
             },
             "StringEquals":{
                "dynamodb:Select":[
                   "SPECIFIC_ATTRIBUTES"
                ]
             }
          }
       }
    ]
}
```

Restricción de la realización de cambios en las configuraciones de VPC

> **Encuesta**
>
> Nos encantaría saber su opinión. 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 servicio ayuda a evitar las desviaciones o modificaciones no intencionadas en la configuración de la VPC. Rechaza las nuevas conexiones de las puertas de enlace de Internet, las conexiones de emparejamiento de VPC, las conexiones de puertas de enlace 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 en su organización, consulte AWS Transit Gateway en esta guía.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
```

```
                "ec2:AttachInternetGateway",
                "ec2:CreateInternetGateway",
                "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

> **Encuesta**
>
> Nos encantaría saber su opinión. 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 en su organización, consulte AWS Enclaves Nitro en esta guía. Para obtener una lista completa de las claves de AWS KMS condición que se pueden usar en las políticas clave y en las políticas AWS Identity and Access Management (de IAM), consulte Claves de condición para. 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
            }
         }
      }
   ]
}
```

Preparación de estrategias para la expansión global

> **Encuesta**
>
> Nos encantaría saber su opinión. Proporcione sus comentarios sobre la AWS PRA mediante una breve encuesta.

AWS A medida que se expande a nivel mundial, Security Assurance Services recibe con frecuencia preguntas sobre cómo diseñar una arquitectura que AWS respete la privacidad. Las preguntas giran en torno a la preocupación por mantener el cumplimiento de los requisitos de privacidad específicos, como las obligaciones de soberanía de datos o los contratos con los clientes, evitando al mismo tiempo costos adicionales y gastos operativos. Las consideraciones sobre el diseño suelen incluir la residencia de datos, la restricción del acceso de los operadores, la resiliencia y la capacidad de supervivencia y la independencia general. Para obtener más información, consulte Cumplir con los requisitos de soberanía digital en AWS(presentación de AWS re:Invent 2022).

Las siguientes preguntas son habituales y solo usted puede responderlas para su caso de uso:

- ¿Dónde deben residir los datos personales de mis clientes?
- ¿Dónde se almacenan los datos de mis clientes?
- ¿Cómo y dónde pueden cruzar fronteras los datos personales?
- ¿El acceso humano o de los servicios a los datos entre regiones se considera una transferencia?
- ¿Cómo puedo estar seguro de que ningún gobierno extranjero pueda acceder a los datos personales de mis clientes?
- ¿Dónde puedo almacenar mis copias de seguridad y los sitios activos o inactivos?
- Para mantener los datos locales, ¿debo mantener una AWS landing zone en cada región en la que ofrezco servicios? ¿O puedo usar una AWS Control Tower landing zone existente?

En cuanto a los requisitos de residencia de datos, las diferentes implementaciones de arquitectura podrían funcionar mejor para diferentes organizaciones. Es posible que algunas organizaciones exijan que los datos personales de los clientes permanezcan en una región específica. Si es así, es posible que quiera saber cómo cumplir con las normativas en general y, al mismo tiempo, cumplir estas obligaciones. Independientemente de la situación, hay varias consideraciones que debe tener en cuenta a la hora de elegir una estrategia para implementar varias cuentas.

Para definir los componentes clave del diseño de la arquitectura, trabaje en estrecha colaboración con los equipos de cumplimiento y contratación para confirmar los requisitos sobre dónde, cuándo y cómo pueden cruzar las Regiones de AWS los datos personales. Determine qué se considera una transferencia de datos: moverlos, copiarlos o verlos. Además, comprenda si hay controles específicos de resiliencia y protección de datos que deban implementarse. ¿Las estrategias de copia de seguridad y recuperación ante desastres requieren una conmutación por error entre regiones? En caso afirmativo, averigüe qué regiones puede usar para almacenar sus datos de copia de seguridad. Determine si hay algún requisito para el cifrado de datos, como un algoritmo de cifrado específico o módulos de seguridad de hardware específicos para la generación de claves. Tras contactar con las partes interesadas en materia de cumplimiento en relación con estos temas, comience a valorar enfoques de diseño para su entorno de varias cuentas.

Los siguientes son tres enfoques que puede utilizar para planificar su estrategia de varias cuentas de AWS , en orden ascendente según la división de la infraestructura:

- Zona de aterrizaje central con regiones administradas
- Zonas de aterrizaje regionales
- AWS Nube soberana europea

También debe recordar que el cumplimiento de la privacidad posiblemente no se limite únicamente a la soberanía de datos. Consulte el resto de esta guía para entender las posibles soluciones a muchos otros desafíos, como la administración del consentimiento, las solicitudes de los titulares de datos, la gobernanza de datos y los sesgos de la IA.

Zona de aterrizaje central con regiones administradas

Si quieres expandirte a nivel mundial pero ya has establecido una arquitectura multicuenta AWS, es habitual que desees utilizar la misma zona de landing multicuenta (MALZ) para gestionar más. Regiones de AWS En esta configuración, seguirías gestionando servicios de infraestructura como el registro, la fábrica de cuentas y la administración general desde tu AWS Control Tower landing zone actual, en la región en la que la creaste.

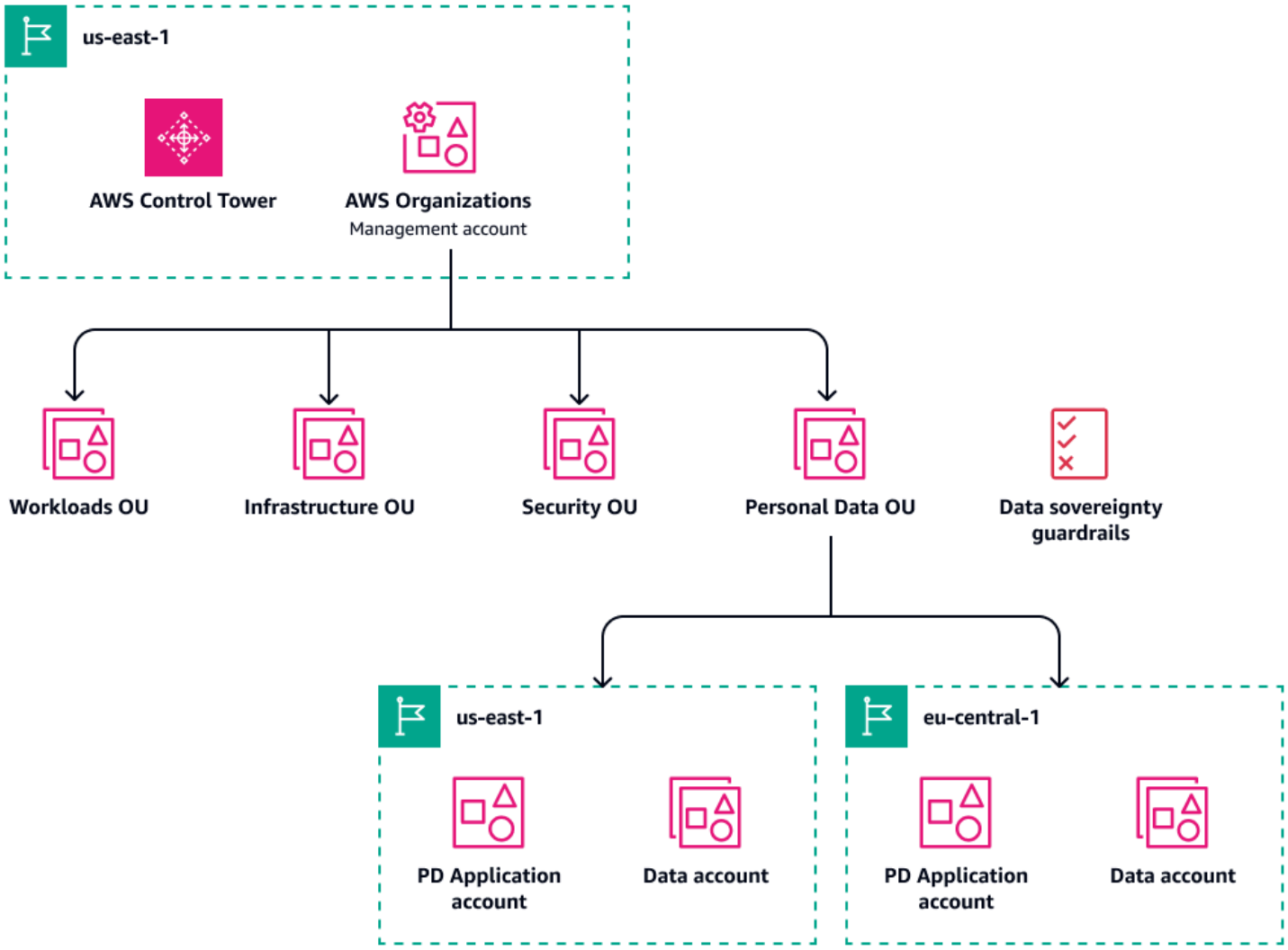
Para las cargas de trabajo de producción, puede realizar implementaciones regionales si amplía la zona de aterrizaje de AWS Control Tower a una nueva región. De este modo, puede ampliar la gobernanza de AWS Control Tower a la nueva región. De esta forma, puede mantener los almacenes de datos personales en una región gestionada específica; los datos seguirán residiendo en cuentas que se benefician de los servicios de infraestructura y la AWS Control Tower gobernanza.

En el caso de las cuentas que contienen datos personales AWS Organizations, se siguen agrupando en una unidad organizativa dedicada a los datos personales, en la que se AWS Control Tower implementan todas las barreras de soberanía de los datos. Además, las cargas de trabajo específicas de cada región se encuentran en cuentas dedicadas, en lugar de establecer cuentas de producción que pueden contener la misma carga de trabajo en varias regiones.

Esta implementación puede ser la más rentable, pero es necesario tener más en cuenta para controlar el flujo de datos personales a través de las fronteras Cuenta de AWS regionales. Considere lo siguiente:

- Los registros pueden contener datos personales, por lo que tal vez necesite alguna configuración adicional para contener o suprimir los campos confidenciales a fin de evitar la transferencia entre regiones durante la agrupación. Para obtener más información y las prácticas recomendadas para controlar la agrupación de registros entre regiones, consulte Almacenamiento de registros centralizado en esta guía.
- En el AWS Transit Gateway diseño, tenga en cuenta el aislamiento VPCs y el flujo de tráfico de red bidireccional adecuado. Puede limitar qué conexiones de puerta de enlace de tránsito están permitidas y aprobadas, y puede limitar quién o qué puede cambiar las tablas de enrutamiento de la VPC.
- Es posible que tenga que impedir que los miembros del equipo de operaciones en la nube accedan a datos personales. Por ejemplo, los registros de aplicaciones que contengan datos de transacciones de clientes pueden considerarse de mayor confidencialidad que otros orígenes del registro. Es posible que necesite más aprobaciones y barreras de protección técnicas, como el control de acceso basado en roles y el control de acceso basado en atributos. Además, los datos pueden estar sujetos a limitaciones de residencia en lo que respecta al acceso. Por ejemplo, solo se puede acceder a los datos de una región A desde esa región.

En el siguiente diagrama se muestra una zona de aterrizaje centralizada con implementaciones regionales.



Zonas de aterrizaje regionales

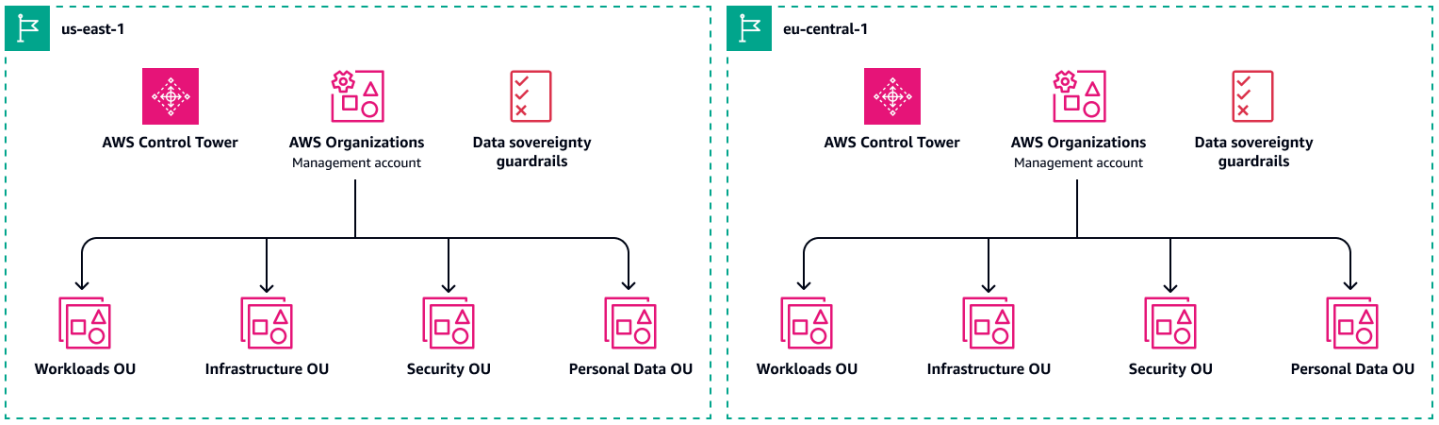
Tener más de un MALZ puede ayudarle a cumplir requisitos de conformidad más estrictos, ya que aísla completamente las cargas de trabajo que procesan datos personales en comparación con las cargas de trabajo no materiales. AWS Control Tower La agregación de registros centralizada podría configurarse de forma predeterminada y, por lo tanto, simplificarse. Con este enfoque, no es necesario que mantenga excepciones para el registro con flujos de registros separados que se tengan que suprimir. Incluso puede tener un equipo de operaciones en la nube local y dedicado para cada MALZ, lo que limita el acceso de los operadores a la residencia local.

Muchas organizaciones tienen implementaciones separadas en las zonas de aterrizaje de EE. UU. y la UE. Cada zona de aterrizaje regional tiene una postura de seguridad única y general y una gobernanza asociada para las cuentas de la región. Por ejemplo, el cifrado de los datos personales

mediante una MALZ específica HSMs puede no ser necesario en las cargas de trabajo de una MALZ, pero puede que sí lo sea en otra MALZ.

Si bien esta estrategia puede ampliarse para cumplir con muchos requisitos actuales y futuros, es importante comprender los costos adicionales y los gastos operativos asociados con el mantenimiento de varios MALZs. Para obtener más información, consulte Precios de AWS Control Tower.

En el siguiente diagrama se muestran zonas de aterrizaje separadas en dos regiones.



AWS Nube soberana europea

Algunas organizaciones necesitan una separación completa para las cargas de trabajo que operan en el Espacio Económico Europeo (EEE) y las cargas de trabajo que operan en otros lugares. En esta situación, considere la posibilidad de usar AWS European Sovereign Cloud. AWS European Sovereign Cloud es una nube nueva e independiente para Europa, que se ha diseñado para ayudar a los clientes a satisfacer las cambiantes necesidades de soberanía de la región, incluidos los estrictos requisitos de residencia de datos, autonomía operativa y resiliencia.

La nube soberana AWS europea está separada física y lógicamente de la existente y Regiones de AWS, al mismo tiempo, ofrece la misma seguridad, disponibilidad y rendimiento. Solo AWS los empleados que se encuentran en la UE tienen el control de las operaciones y el soporte de la nube soberana AWS europea. Si tiene requisitos estrictos de residencia de datos, la Nube Soberana AWS Europea conserva todos los metadatos que cree (como las funciones, los permisos, las etiquetas de los recursos y las configuraciones que utilizan para ejecutarse AWS) en la UE. La nube soberana AWS europea también cuenta con sus propios sistemas de facturación y medición del uso.

Para este enfoque, utilizaría un patrón similar al de la sección anterior, las zonas de aterrizaje regionales. Sin embargo, en el caso de los servicios que presta a clientes europeos, puede implementar un MALZ dedicado en la nube soberana AWS europea.

Recursos

> **Encuesta**
>
> Nos encantaría saber su opinión. Responda a una breve encuesta para enviar sus comentarios sobre AWS PRA.

Recomendaciones de AWS

- Arquitectura de referencia de seguridad de AWSAWS (SRA de)

AWSDocumentación de

- Protección de los datos (Marco de AWS Well-Architected)
- Data classification (documento técnico de AWS)
- Amazon Web Services: Risk and Compliance (documento técnico de AWS)
- Hybrid architectures to address personal data processing requirements (documento técnico de AWS)
- Navigating GDPR Compliance on AWS (documento técnico de AWS)
- Building a data perimeter on AWS (documento técnico de AWS)
- Documentación de seguridad de AWS

Otros recursos de AWS

- Programas de conformidad de AWS
- AWS Modelo de responsabilidad compartida de
- Preguntas frecuentes sobre privacidad de datos
- AWS Security Assurance Services
- AWS Digital Sovereignty Pledge: Control without compromise (entrada en el blog de AWS)
- AWS Security Learning

Colaboradores

> **Encuesta**
>
> Nos encantaría saber su opinión. Responda a una breve encuesta para enviar sus comentarios sobre AWS PRA.

El autor de esta guía es el equipo de AWS Security Assurance Services. Si necesita ayuda para implementar las recomendaciones de esta guía y poner en funcionamiento las cargas de trabajo, contacte con el equipo de AWS Security Assurance Services.

Autores principales

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

Colaboradores

- Avik Mukherjee, consultor sénior de seguridad de AWS
- David Bounds, arquitecto sénior de soluciones de AWS
- Jeff Lombardo, arquitecto sénior de soluciones de seguridad de AWS
- Ram Ramani, arquitecto principal de soluciones de seguridad de AWS
- Vanessa Jacobs, consultora sénior de seguridad de AWS
- Thomas Nicholson, consultor sénior de privacidad de AWS
- Jose DeJesus, consultor sénior de garantías de AWS
- Doug Pardue, gerente de arquitectura de soluciones de AWS

Autores técnicos

- Lilly AbouHarb, redactora técnica sénior de AWS

Historial de documentos

> **Encuesta**
>
> Nos encantaría saber su opinión. Responda a una breve encuesta para enviar sus comentarios sobre AWS PRA.

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	Agregamos el Catálogo de controles de cumplimiento de la computación en la nube (C5) a la sección AWS Artifact. Agregamos Amazon Security Lake a la cuenta de archivos de registro. Agregamos Amazon Bedrock, AWS Clean Rooms, Amazon DataZone, AWS Lake Formation, Amazon SageMaker AI y caracterí sticas y Servicios de AWS que ayudan a detectar, clasificar o catalogar datos a la cuenta de la aplicación de datos personales. Agregamos la sección Preparación de estrategias para la expansión global.	16 de septiembre de 2025
Actualizaciones importantes	Hicimos actualizaciones importantes en todo el documento.	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:

- Refactor/re-architect — Mueva una aplicación y modifique su arquitectura aprovechando al máximo las funciones nativas de 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 PostgreSQL-Compatible edición 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: Migrar la base de datos Oracle en las instalaciones a Amazon Relational Database Service (Amazon RDS) para Oracle en la nube de 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 hacer cambios para aprovechar las funcionalidades de la nube. Ejemplo: Migrar la base de datos de Oracle en las instalaciones a Oracle en una instancia de EC2 en la Nube de AWS.
- Reubicar: (migrar el hipervisor mediante lift and shift): traslade la infraestructura a la nube sin comprar equipo nuevo, reescribir aplicaciones o modificar las operaciones actuales. Los servidores se migran de una plataforma en las instalaciones 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

A2A () Agent-to-Agent

Un protocolo completo para la colaboración entre agentes que facilita la delegación de tareas y la transferencia de estados.

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios administrados.

ACID

Consulte atomicidad, consistencia, aislamiento, 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 una 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 de origen gestiona las transacciones de las aplicaciones conectadas, mientras los datos se replican en la de destino. La base de datos de destino no acepta ninguna transacción durante la migración.

Agente

Un sistema de IA que puede razonar, planificar y tomar medidas de forma autónoma utilizando herramientas para alcanzar los objetivos.

Agent Ops

Prácticas operativas para crear, probar, implementar y ejecutar agentes de IA en producción a escala.

función de agregación

Función SQL que actúa en un grupo de filas y calcula un único valor de devolución para el grupo. Entre los ejemplos de funciones de agregación se incluyen `SUM` y `MAX`.

IA

Consulte inteligencia artificial.

AIOps

Consulte 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

Enfoque de seguridad que permite usar de manera exclusiva aplicaciones aprobadas para ayudar a proteger un sistema contra el malware.

cartera de aplicaciones

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

inteligencia artificial (IA)

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

operaciones de inteligencia artificial (AIOps)

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

cifrado asimétrico

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

atomicidad, consistencia, aislamiento, durabilidad (ACID)

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

control de acceso basado en atributos (ABAC)

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

origen de datos fidedigno

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

Zona de disponibilidad

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

AWS Marco de adopción de la nube (AWS CAF)

Un marco de directrices y mejores prácticas AWS para ayudar a las organizaciones a desarrollar un plan eficiente y eficaz para migrar con éxito a la nube. AWS CAF organiza la orientación en seis áreas de enfoque denominadas perspectivas: negocios, personas, gobierno, plataforma, seguridad y operaciones. Las perspectivas empresariales, humanas y de gobernanza se centran en las habilidades y los procesos empresariales; las perspectivas de plataforma, seguridad y

operaciones se centran en las habilidades y los procesos técnicos. Por ejemplo, la perspectiva humana se dirige a las partes interesadas que se ocupan de los Recursos Humanos (RR. HH.), las funciones del personal y la administración de las personas. Desde esta perspectiva, AWS CAF proporciona orientación para el desarrollo, la formación y la comunicación de las personas a fin de preparar a la organización para una adopción exitosa de la nube. Para obtener más información, consulte la Página web de AWS CAF y el Documento técnico de AWS CAF.

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

Herramienta que evalúa las cargas de trabajo de migración de bases de datos, recomienda estrategias de migración y proporciona estimaciones de trabajo. AWS WQF se incluye con AWS Schema Conversion Tool ().AWS SCT Analiza los esquemas de bases de datos y los objetos de código, el código de las aplicaciones, las dependencias y las características de rendimiento y proporciona informes de evaluación.

B

bot malicioso

Bot destinado a causar interrupciones o daños a personas u organizaciones.

BCP

Consulte 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. Consulte también endianidad.

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.

blue/green despliegue

Estrategia de implementación 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 se ejecuta en el otro entorno (verde). Esta estrategia lo ayuda a hacer reversiones rápidas 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 la información de Internet. Otros bots, conocidos como bots maliciosos, tienen como objetivo causar interrupciones o daños a personas u organizaciones.

botnet

Redes de bots infectadas por malware y que están bajo el control de una sola parte, conocida como pastor de bots 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 de emergencia

En circunstancias excepcionales y mediante un proceso aprobado, es una forma rápida de que un usuario pueda acceder a un Cuenta de AWS sitio al que normalmente no tiene permisos de acceso. Para obtener más información, consulte el indicador de implementación de procedimientos rompe-cristales en la AWS Well-Architected guía.

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 AWS Cloud Adoption Framework.

implementación canario

Lanzamiento lento e incremental de una versión para los usuarios finales. Cuando tenga mayor confianza en la nueva versión, la implementa y reemplaza la versión actual en su totalidad.

CCoE

Consulte Centro de excelencia en la nube.

CDC

Consulte 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

Introducción intencionada de 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 integración continua y 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.

Desarrollador ciudadano

Un usuario empresarial que crea aplicaciones de IA utilizando plataformas sin code/low código sin conocimientos técnicos especializados.

cifrado del cliente

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

Centro de excelencia en la nube (CCoE)

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

computación en la nube

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

modelo operativo en la nube

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

etapas de adopción de la nube

Las siguientes son las cuatro fases por las que suelen pasar las empresas cuando migran a la Nube de AWS:

- Proyecto: ejecución de algunos proyectos relacionados con la nube con fines de prueba de concepto y aprendizaje
- Fundamento: realización de inversiones fundamentales para escalar la adopción de la nube (p. ej., crear una zona de aterrizaje, definir un CCoE, establecer un modelo de operaciones)
- Migración: migración de aplicaciones individuales
- Re-invention — Optimizar los productos y servicios e innovar en la nube

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

CMDB

Consulte base de datos de administración de 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. Algunos repositorios en la nube comunes son GitHub o Bitbucket Cloud. Cada versión del código se denomina rama. En una estructura de microservicios, cada repositorio se encuentra dedicado a una única funcionalidad. Una sola CI/CD canalización 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 machine learning para analizar y extraer información de formatos visuales, como imágenes y videos digitales. Por ejemplo, Amazon SageMaker AI proporciona algoritmos de procesamiento de imágenes para CV.

deriva de configuración

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

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

Un conjunto de AWS Config reglas y medidas correctivas que puede reunir para personalizar sus controles 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, creación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD se describe comúnmente como una canalización. CI/CD puede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar más rápido. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Consulte visión artificial.

D

datos en reposo

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

clasificación de datos

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

deriva 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 deriva de 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

Marco de arquitectura que proporciona una propiedad de datos distribuida y descentralizada con una administración y una gobernanza centralizadas.

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

Sistema de administración de datos que respalda la inteligencia empresarial, como los análisis. Los almacenes de datos suelen contener grandes cantidades de datos históricos y, por lo general, se utilizan para las consultas y los 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 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.

defensa en profundidad

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 enfoque de defensa en profundidad podría combinar la autenticación multifactor, 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 en 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 suelen utilizar para restringir consultas, filtrarlas y etiquetar los 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)

Estrategia y proceso que utiliza para minimizar el tiempo de inactividad y la pérdida de datos a causa de un desastre. Para obtener más información, consulte Recuperación de cargas de trabajo ante desastres en AWS: Recuperación en la nube en el AWS Well-Architected marco.

DML

Consulte 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. Eric Evans introdujo este concepto en su libro Domain-Driven Design: Tackling Complexity in the Heart of 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 ASP.NET Microsoft (ASMX) mediante contenedores y Amazon API Gateway.

DR

Consulte recuperación ante desastres.

Detección de desviaciones

Seguimiento de las desviaciones con respecto a una configuración con línea de base. 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 asignación de flujos de valor para el desarrollo.

E

EDA

Consulte análisis de datos de tipo exploratorio.

EDI

Consulte 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 la nube, la computación de periferia puede reducir la latencia de la comunicación y mejorar el tiempo de respuesta.

intercambio electrónico de datos (EDI)

Intercambio automatizado de documentos comerciales entre organizaciones. Para más información, consulte ¿Qué es el intercambio electrónico de datos?

cifrado

Proceso de computación que transforma datos de texto plano, que son 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. Big-endian los sistemas almacenan primero el byte más significativo. Little-endian los sistemas almacenan primero el byte menos significativo.

punto de conexión

Consulte punto de conexión de 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 con AWS PrivateLink entidades principales Cuentas de AWS o AWS Identity and Access Management (de IAM) y conceder permisos a ellas. 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)

Sistema que automatiza y administra los procesos empresariales clave (como la contabilidad, MES y la administración de proyectos) de una empresa.

cifrado de sobre

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

entorno

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

- entorno de desarrollo: instancia de una aplicación en ejecución que solo se encuentra disponible para el equipo principal responsable del mantenimiento de la aplicación. Los entornos de desarrollo se utilizan para probar los cambios antes de promocionarlos a los entornos superiores. Este tipo de entorno a veces se denomina entorno de prueba.
- entornos inferiores: todos los entornos de desarrollo de una aplicación, como los que se utilizan para las compilaciones y pruebas iniciales.

- entorno de producción: instancia de una aplicación en ejecución a la que pueden acceder los usuarios finales. En un CI/CD proceso, el entorno de producción es el último entorno de implementación.
- entornos superiores: todos los entornos a los que pueden acceder usuarios que no sean del equipo de desarrollo principal. Esto puede incluir un entorno de producción, entornos de preproducción y entornos para las pruebas de aceptación por parte de los usuarios.

epopeya

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

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 hechos

Tabla central de un esquema en estrella. Almacena datos cuantitativos sobre operaciones empresariales. Por lo general, 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.

Fail Fast

Filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo. Es una parte fundamental de los enfoques ágiles.

límite de aislamiento de errores

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 más información, consulte AWS Fault Isolation Boundaries.

rama de característica

Consulte rama.

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.

peticiones con pocos pasos

Proporcionar a un LLM una pequeña cantidad de ejemplos que demuestren la tarea y el resultado deseado antes de pedirle que lleve a cabo una tarea similar. Esta técnica es una aplicación del aprendizaje contextual, en el que los modelos aprenden a partir de ejemplos (tomas) integrados en las instrucciones. Few-shot Las indicaciones pueden ser eficaces para tareas que requieren un formato, un razonamiento o un conocimiento del dominio específicos. Consulte también peticiones desde cero.

FGAC

Consulte 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 de cambio 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 modelo fundacional.

Modelo fundacional (FM)

Gran red neuronal de aprendizaje profundo que se entrenó con conjuntos de datos masivos de datos generalizados y no etiquetados. Los FM pueden hacer una amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes y conversar en lenguaje natural. Para más información, consulte ¿Qué son los modelos fundacionales?

Puerta de enlace FM

Un intermediario centralizado que controla y normaliza el acceso a los modelos básicos. También se conoce como puerta de enlace LLM.

G

IA generativa

Subconjunto de modelos de IA que se entrenaron con grandes cantidades de datos y que pueden utilizar una simple petición de texto para crear contenido y artefactos nuevos, como imágenes, videos, texto y audio. Para más información, consulte ¿Qué es la IA generativa?

bloqueo geográfico

Consulte 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, mientras que el flujo de trabajo basado en enlaces troncales es el enfoque moderno preferido.

imagen dorada

Instantánea de un sistema o software que se usa 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 la conformidad en todas las unidades organizativas (OU). Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de permisos de IAM. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

barandas (AI)

Mecanismos de seguridad que filtran, validan y restringen las entradas y salidas de los agentes para ayudar a garantizar un comportamiento responsable y seguro de la IA.

H

HA

Consulte alta disponibilidad.

migración heterogénea de bases de datos

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

alta disponibilidad (HA)

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

modernización histórica

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

datos de reserva

Parte de los datos históricos etiquetados que se ocultan de un conjunto de datos que se utiliza para entrenar un modelo de machine learning. Puede utilizar los datos de reserva para evaluar el rendimiento del modelo mediante la comparación de las predicciones del modelo con los datos de reserva.

human-in-the-loop (HiTL)

Un patrón de flujo de trabajo en el que la ejecución de los agentes se detiene para su revisión y aprobación por parte de una persona en los puntos de decisión críticos.

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, una revisión suele realizarse fuera del flujo de trabajo habitual de las DevOps versiones.

periodo de hiperatención

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

I

IaC

Consulte infraestructura como código.

políticas basadas en identidades

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

aplicación inactiva

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

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

Modelo que implementa una nueva infraestructura para las cargas de trabajo de producción en lugar de actualizar o modificar la infraestructura existente o aplicarle revisiones. Las infraestructuras inmutables son de manera intrínseca más coherentes, fiables y predecibles que las infraestructuras mutables. Para obtener más información, consulte las mejores prácticas del Framework para implementar con una infraestructura inmutable. AWS Well-Architected

VPC entrante (de entrada)

En una arquitectura de AWS cuentas múltiples, una VPC que acepta, inspecciona y enruta las conexiones de red desde fuera de una aplicación. La Arquitectura de referencia de seguridad de AWS recomienda configurar su cuenta de red con VPC entrantes, salientes y de inspección para proteger la interfaz bidireccional entre su aplicación e Internet en general.

migración gradual

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

Industria 4.0

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

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial (IIoT)

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

VPC de inspección

En una arquitectura de AWS cuentas múltiples, una VPC centralizada que gestiona las inspecciones del tráfico de red entre las VPC (iguales o Regiones de AWS diferentes), Internet y las redes locales. La Arquitectura de referencia de seguridad de AWS recomienda configurar su

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

Internet de las cosas (IoT)

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

interpretabilidad

Característica de un modelo de machine learning que describe el grado en que un ser humano puede entender cómo las predicciones del modelo dependen de sus entradas. Para 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 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 de gran tamaño (LLM)

Modelo de IA de aprendizaje profundo que se entrenó previamente con una gran cantidad de datos. Un LLM puede llevar a cabo varias tareas, como responder preguntas, resumir documentos, traducir textos a otros idiomas y completar oraciones. Para más información, consulte ¿Qué es un LLM (modelo de lenguaje de gran tamaño)?

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

Consulte Las 7 R.

sistema little-endian

Un sistema que almacena primero el byte menos significativo. Consulte también endianidad.

LLM

Consulte modelo de lenguaje de gran tamaño.

entornos inferiores

Consulte 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

Consulte rama.

malware

Software diseñado para comprometer la seguridad o la privacidad de la computadora. El malware podría 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 administrados

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

sistema de ejecución de fabricación (MES)

Sistema de software para seguir, supervisar, documentar y controlar los procesos de producción que convierten las materias primas en productos acabados en la zona de producción.

MAP

Consulte Programa de aceleración de la migración.

MCP

Consulte Model Context Protocol.

Protocolo de contexto para modelos (MCP)

Un protocolo sin estado para la comunicación entre el agente y la herramienta.

Servidor MCP

Un servicio que expone una o más herramientas a través del protocolo Model Context.

mecanismo

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

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 sistema de ejecución de fabricación.

Message Queuing Telemetry Transport (MQTT)

Un protocolo de comunicación ligero de máquina a máquina (M2M), basado en el publish/subscribepatrón, para dispositivos de IoT con recursos limitados.

microservicio

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

arquitectura de microservicios

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

Programa de aceleración de la migración (MAP)

Un AWS programa que proporciona soporte de consultoría, formación y servicios para ayudar a las organizaciones a crear una base operativa sólida para migrar a la nube y para ayudar a

compensar el costo inicial de las migraciones. El MAP incluye una metodología de migración para ejecutar las migraciones antiguas de forma metódica y un conjunto de herramientas para automatizar y acelerar los escenarios de migración más comunes.

migración a escala

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

fábrica de migración

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

metadatos de migración

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

patrón de migración

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

Migration Portfolio Assessment (MPA)

Herramienta en línea que proporciona información a fin de validar los argumentos comerciales necesarios para migrar a la Nube de AWS. La MPA ofrece una evaluación detallada de la cartera (adecuación del tamaño de los servidores, precios, comparaciones del costo total de propiedad, análisis de los costos de migración), así como una planificación de la migración (análisis y recopilación de datos de aplicaciones, agrupación de aplicaciones, priorización de la migración y

planificación de oleadas). La herramienta MPA (requiere iniciar sesión) está disponible de forma gratuita para todos los AWS consultores y consultores de los socios 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

Enfoque utilizado para migrar una carga de trabajo a la Nube de AWS. Para más información, consulte la entrada Las 7 R de este glosario y también Mobilize your organization to accelerate large-scale migrations.

ML

Consulte machine learning.

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 más información, consulte Strategy for modernizing applications in the 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 más información, consulte Evaluating modernization readiness for applications in the Nube de AWS.

aplicaciones monolíticas (monolitos)

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

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

MPA

Consulte Migration Portfolio Assessment.

MQTT

Consulte Message Queuing Telemetry Transport.

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

Modelo que actualiza y modifica la infraestructura actual para las cargas de trabajo de producción. Para mejorar la coherencia, la confiabilidad y la previsibilidad, el AWS Well-Architected Marco recomienda el uso de una infraestructura inmutable como práctica recomendada.

O

OAC

Consulte control de acceso de origen.

OAI

Consulte identidad de acceso de origen.

OCM

Consulte administración del cambio organizacional.

migración fuera de línea

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

OI

Consulte integración de operaciones.

OLA

Consulte acuerdo de 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 de máquina a máquina (M2M) para la automatización industrial. 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)

Lista de comprobación de preguntas y prácticas recomendadas asociadas que son útiles para comprender, evaluar, prevenir o reducir el alcance de los incidentes y posibles errores. Para obtener más información, consulte las revisiones de preparación operativa (ORR) en el AWS Well-Architected marco.

tecnología operativa (TO)

Sistemas de hardware y software que funcionan con el entorno físico para controlar las operaciones, los equipos y la infraestructura industriales. En el sector de la fabricación, 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 y AWS CloudTrail que registra todos los eventos Cuentas de AWS 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 con AWS KMS (SSE-KMS) y `DELETE` las solicitudes `PUT` y dinámicas al bucket de S3.

identidad de acceso de origen (OAI)

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

ORR

Consulte revisión de la preparación operativa.

OT

Consulte tecnología operativa.

VPC saliente (de salida)

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

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

P

límite de permisos

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

información de identificación personal (PII)

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

PII

Consulte 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 administración del ciclo de vida del producto.

policy

Objeto que puede definir permisos (consulte política basada en identidad), especificar las condiciones de acceso (consulte política basada en recursos) o definir los permisos máximos para todas las cuentas de una organización de AWS Organizations (consulte política de control de servicio).

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.

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

Condición de consulta que devuelve `true` o `false`. En general, se encuentra en una cláusula `WHERE`.

inserción de predicados

Técnica de optimización de consultas en bases de datos que filtra los datos de la consulta antes de transferirlos. Esta técnica reduce la cantidad de datos de la base de datos relacional que se tienen que recuperar y procesar. Además, 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

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

zonas alojadas privadas

Contenedor que aloja información acerca de cómo desea que responda Amazon Route 53 a las consultas de DNS de un dominio y sus subdominios en una o varias VPC. Para obtener más información, consulte Uso de zonas alojadas privadas en la documentación de Route 53.

control proactivo

Control de seguridad que se diseñó para evitar la implementación de recursos que no cumplan con la normativa. Estos controles analizan los recursos antes de aprovisionarlos. Si el recurso no cumple con los requisitos del control, no se aprovisiona. 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.

administración del ciclo de vida del producto (PLM)

Administración 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 la reducción de su uso y su retirada.

entorno de producción

Consulte entorno.

controlador lógico programable (PLC)

En el sector de la fabricación, computadora adaptable y altamente fiable que supervisa las máquinas y automatiza los procesos de fabricación.

encadenamiento de peticiones

Uso de la salida de una petición de LLM como entrada para la siguiente petición a fin de generar mejores respuestas. Esta técnica se utiliza para dividir una tarea compleja en tareas secundarias 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)

Patrón que permite establecer 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 pueden suscribir otros microservicios. El sistema puede agregar 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

Consulte responsable, fiable, consultada e informada (RACI).

RAG

Consulte generación aumentada por recuperación.

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

Consulte responsable, fiable, consultada e informada (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

Consulte Las 7 R.

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

Consulte Las 7 R.

Region

Conjunto 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 más información, consulte Specify which Regiones de AWS your account can use.

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 Las 7 R.

versión

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

reubicar

Consulte Las 7 R.

redefinir la plataforma

Consulte Las 7 R.

recomprar

Consulte Las 7 R.

resiliencia

Capacidad de una aplicación para resistir interrupciones o recuperarse de ellas. Al planificar la resiliencia en la Nube de AWS, la alta disponibilidad y la recuperación ante desastres son consideraciones comunes. Para más información, consulte Resiliencia en la Nube de AWS.

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 Las 7 R.

retirar

Consulte Las 7 R.

Generación aumentada de recuperación (RAG)

Tecnología de IA generativa mediante la que un LLM hace referencia a un origen de datos autorizado que se encuentra fuera de sus orígenes de datos de entrenamiento antes de generar una respuesta. Por ejemplo, un modelo de RAG podría hacer una búsqueda semántica en la base de conocimientos o en los datos personalizados de una organización. Para más información, consulte ¿Qué es RAG (generación aumentada por recuperación)?

rotación

Proceso mediante el que periódicamente se actualiza un secreto para que resulte más difícil que un atacante pueda acceder 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 objetivo de punto de recuperación.

RTO

Consulte 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 Consola de administración de AWS 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 control de supervisión y adquisición de datos.

SCP

Consulte política de control de servicio.

secreta

En AWS Secrets Manager, información confidencial o restringida, como una contraseña o credenciales de usuario, que se almacena de forma cifrada. Se compone del valor del secreto y de sus metadatos. El valor del secreto puede ser binario, una sola cadena o varias cadenas. Para más información, consulte What's in a Secrets Manager secret? en la documentación de Secrets Manager.

seguridad desde el diseño

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 de controles de seguridad principales: preventivos, de detección, de respuesta y proactivos.

refuerzo de la seguridad

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

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

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

automatización de la respuesta de seguridad

Acción predefinida y programada que está diseñada para responder automáticamente a un evento de seguridad o corregirlo. Estas automatizaciones sirven como controles de seguridad

preventivos o adaptables que le ayudan a implementar las mejores prácticas AWS de seguridad. La modificación de un grupo de seguridad de VPC, la aplicación de revisiones a una instancia de Amazon EC2 o la rotación de credenciales son algunos ejemplos de acciones de respuesta automatizadas.

cifrado del servidor

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

política de control de servicio (SCP)

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

punto de enlace de servicio

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

acuerdo de nivel de servicio (SLA)

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

indicador de nivel de servicio (SLI)

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

objetivo de nivel de servicio (SLO)

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 con AWS la que compartes la seguridad y 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.

Shadow AI

Aplicaciones de IA no autorizadas creadas o utilizadas fuera de los canales regulados dentro de una organización.

SIEM

Consulte sistema de administración de eventos e información de seguridad.

único punto de error (SPOF)

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

SLA

Consulte acuerdo de nivel de servicio.

SLI

Consulte indicador de nivel de servicio.

SLO

Consulte objetivo de nivel de servicio.

modelo de dividir y sembrar

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 más información, consulte Phased approach to modernizing applications in the Nube de AWS.

SPOF

Consulte único punto de error.

esquema en estrella

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

patrón de higo estrangulador

Un enfoque para modernizar los sistemas monolíticos mediante la reescritura y el reemplazo gradual de las funciones del sistema hasta que se pueda desmantelar el sistema heredado.

Este patrón utiliza la analogía de una higuera que crece hasta convertirse en un árbol estable y, finalmente, se apodera y reemplaza a su host. El patrón fue presentado por Martin Fowler como una forma de gestionar el riesgo al reescribir sistemas monolíticos. Para ver un ejemplo de cómo aplicar este patrón, 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.

control de supervisión y adquisición de datos (SCADA)

En el sector de la fabricación, sistema que utiliza hardware y software para supervisar 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

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

petición del sistema

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

T

etiquetas

Key-value pares que actúan como metadatos para organizar sus AWS recursos. Las etiquetas pueden ayudar a administrar, identificar, organizar, buscar y filtrar recursos de . 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.

herramienta

Una función o API que un agente puede invocar para realizar operaciones en sistemas externos.

puerta de enlace de tránsito

Centro de tránsito de red que puede utilizar para interconectar las VPC y las redes en las instalaciones. Para obtener más información, consulte Qué es una pasarela de tránsito en la AWS Transit Gateway documentación.

flujo de trabajo basado en enlaces troncales

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

acceso de confianza

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

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

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

Consulte entorno.

V

succión

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

control de versión

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

Emparejamiento de VPC

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

vulnerabilidad

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

W

caché caliente

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

datos templados

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

función de ventana

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

carga de trabajo

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

flujo de trabajo

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

WORM

Consulte escritura única y lectura múltiple.

WQF

Consulte AWS Workload Qualification Framework.

escritura única y lectura múltiple (WORM)

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

Z

ataque de día cero

Ataque, normalmente de malware, que se aprovecha de 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.

peticiones desde cero

Proporcionar a un LLM instrucciones para llevar a cabo una tarea, pero sin ejemplos (pasos) que puedan ayudar a guiarlo. El LLM debe usar los conocimientos del entrenamiento previo para

llevar a cabo la tarea. La eficacia de la petición desde cero depende de la complejidad de la tarea y de la calidad de la petición. Consulte también peticiones con 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.