Arrastre, camine y corra: acelerando la madurez de la seguridad en Nube de AWS

AWS Orientación prescriptiva

AWS Orientación prescriptiva: Arrastre, camine y corra: acelerando la madurez de la seguridad en Nube de AWS

Table of Contents

Arrastre, camine y corra: acelerando la madurez de la seguridad en Nube de AWS

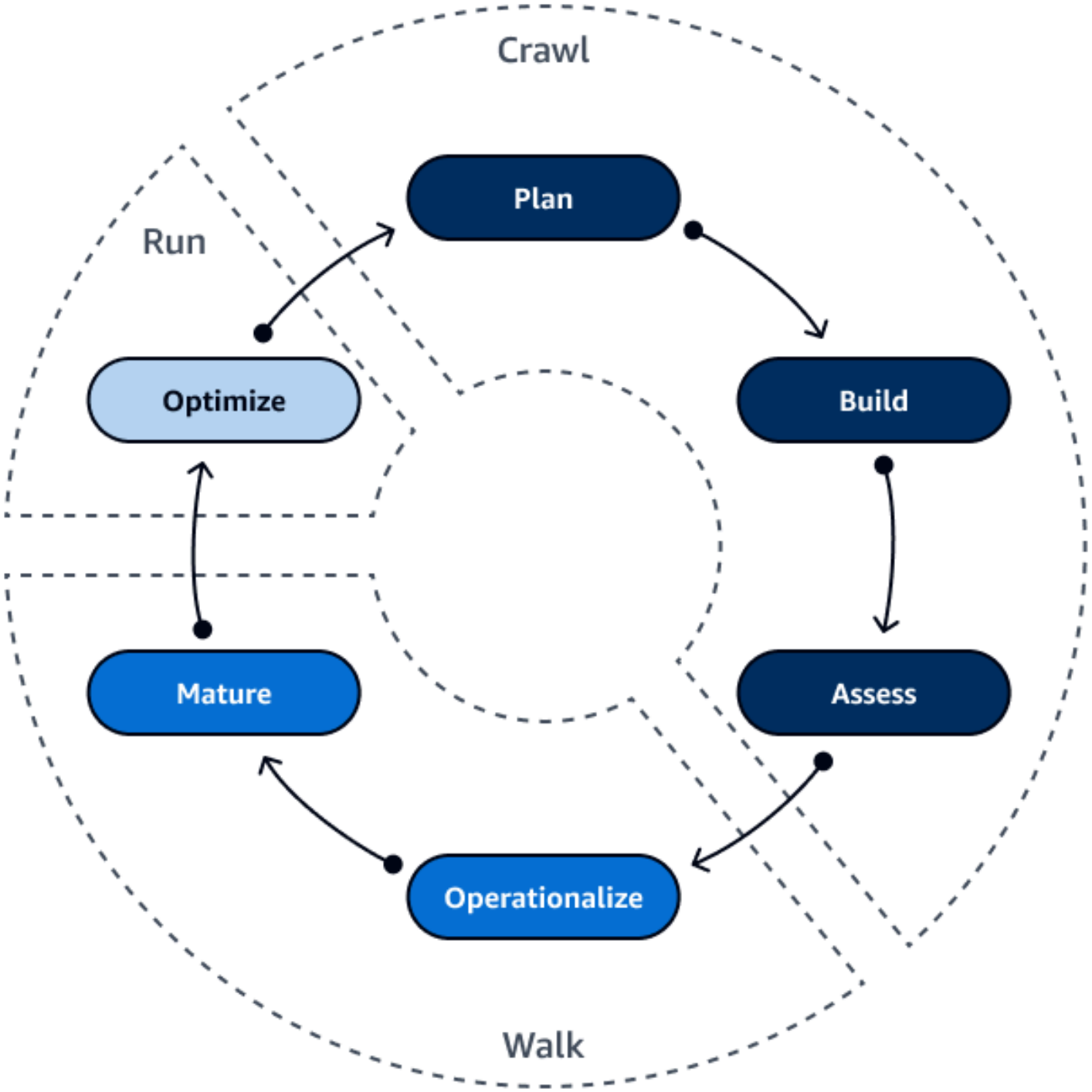
Amazon Web Services (colaboradores)

Diciembre de 2023 (historial de documentos)

Para muchas organizaciones, la seguridad es la prioridad y consideración principal al migrar a la nube. La implementación de capacidades y controles de seguridad en la nube no es una actividad que se efectúe una sola vez, sino que se trata de un modelo iterativo. Aumenta gradualmente la posición de seguridad y su madurez a medida que aumenta las operaciones en la nube. Por ejemplo, puede comenzar con políticas administradas de AWS y, a continuación, cuando su organización esté preparada, puede implementar políticas personalizadas que sigan el principio de privilegio mínimo.

Esta guía proporciona una hoja de ruta para usar la metodología de gatear, caminar y correr para acelerar la madurez de la organización en materia de seguridad de nube. Define un step-by-step enfoque para automatizar las capacidades de seguridad. También explica de forma pragmática cómo aprovechar al máximo las funcionalidades Servicios de AWS y características. Esta guía le ayuda a comprender los desafíos y las oportunidades de la nube y a saber cómo avanzar rápidamente y alcanzar el éxito con ella. AWS

El traspaso a la nube requiere la creación de marcos, la administración y la madurez de las operaciones y la optimización de los procesos. En la siguiente imagen se muestra las fases de cada etapa de la metodología de gatear, caminar y correr: planificación, creación, evaluación, operación, madurez y optimización.



La etapa de gatear consiste en planificar, sentar las bases y evaluar la posición de seguridad actual. En la etapa de caminar, se inician las operaciones de las personas, los procesos y la tecnología y, a continuación, se maduran las operaciones mediante el ajuste y la medición. La etapa de correr consiste en la optimización mediante la evaluación y la automatización.

Etapa de gatear: planificación, creación y evaluación

La etapa de gatear comienza con la planificación. La planificación implica determinar el alcance de seguridad y elegir el modelo que se adapte mejor a la organización. Una vez establecido el plan, puede comenzar a sentar las bases. A continuación, se evalúa la posición de seguridad actual y se establece una disciplina tan pronto como se cree la infraestructura de seguridad. La etapa de gatear es iterativa. La iteración en la nube es más rápida que la iteración en un entorno en las instalaciones. A medida que desarrolla las capacidades en la nube, se acelera el proceso de iteración.

A continuación se muestran las fases de la etapa de gatear:

- Plan: ¿cómo determinará el alcance y seleccionará un modelo?
- Build: ¿cómo establecerá el marco?
- Evaluación: ¿cuál es la posición de seguridad actual?

Planificación: establecimiento del alcance y el modelo de seguridad

La planificación es un proceso iterativo que se produce a medida que va madura el modelo de seguridad. Los pasos clave del proceso de planificación incluyen los siguientes:

- Descripción del alcance de seguridad: el alcance de seguridad varía y depende de cómo se utiliza la nube.
- Elección de un modelo de seguridad: identifique el modelo de seguridad que mejor se adapte a su caso de uso de seguridad.
- Creación de un modelo de objetivos empresariales: defina objetivos y mecanismos claros para medir el éxito.

A medida que desarrolla el plan, tenga en cuenta lo siguiente:

- Debe tener la predisposición para iterar. La iteración es constante en la nube. La iteración lo ayuda a identificar las deficiencias del plan.

- No comience con los servicios. Comience con el plan en lugar de elegir qué servicios necesita. Esto ayuda a que la organización logre los resultados esperados.

Descripción del alcance de seguridad

El modelo de responsabilidad AWS compartida define cómo se comparte la responsabilidad en materia de seguridad y cumplimiento en la nube. AWS AWS protege la infraestructura en la que se ejecutan todos los servicios que se ofrecen en ella Nube de AWS, y usted es responsable de proteger el uso de esos servicios, como sus datos y aplicaciones.

Este modelo compartido puede ayudar a liberar la carga operativa, porque AWS opera, administra y controla muchos componentes, desde el sistema operativo host y la capa de virtualización hasta la seguridad física en las instalaciones en las que opera el servicio. Los servicios gestionados le ayudan a reducir sus obligaciones de seguridad y conformidad, ya que AWS le permiten gestionar algunas tareas de seguridad, como la administración de parches y vulnerabilidades. El uso de servicios administrados es una práctica recomendada en el Marco de AWS Well-Architected. En general, a medida que se moderniza la infraestructura, se transfiere más responsabilidad al proveedor de servicios.

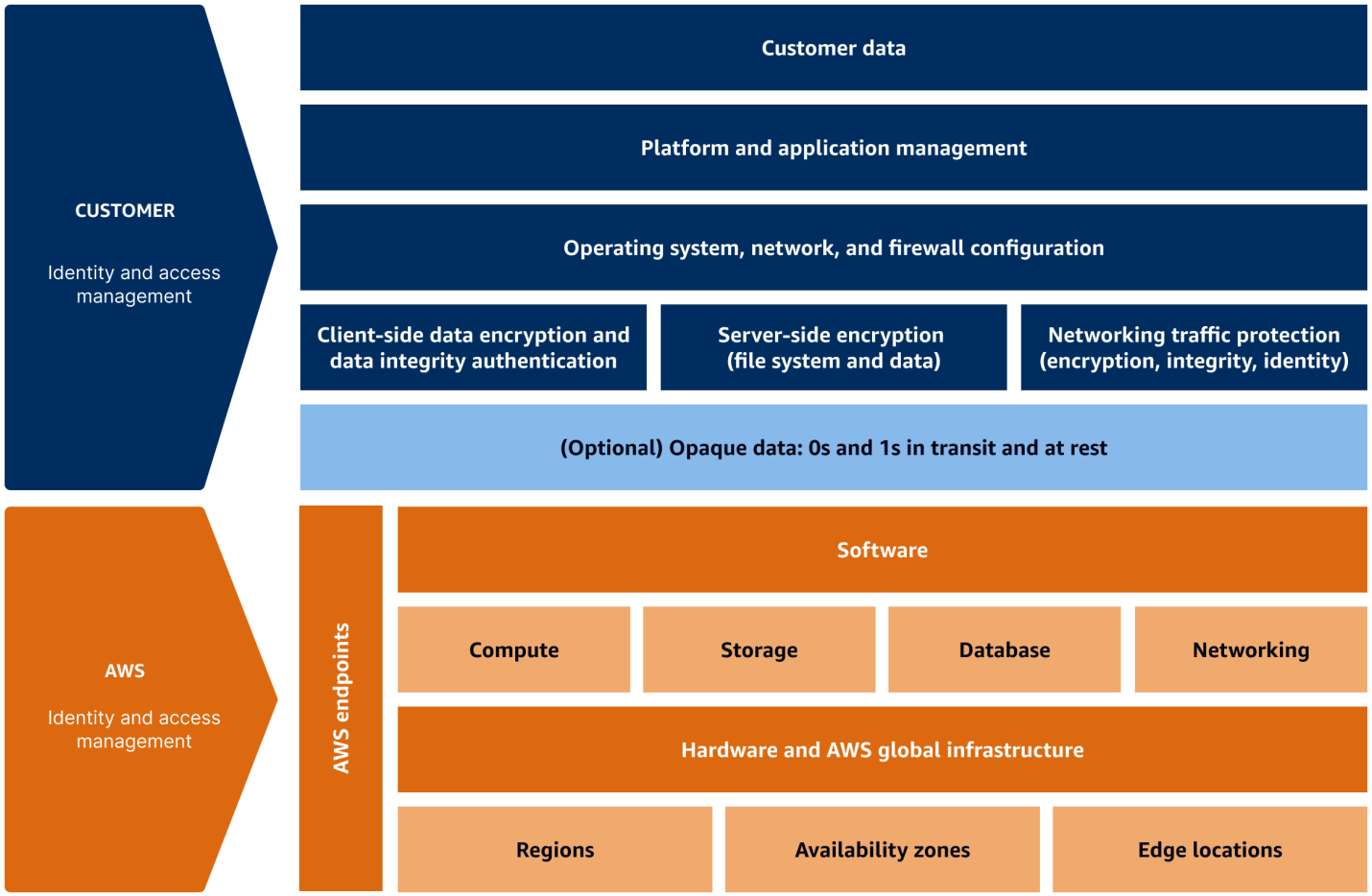
A continuación se muestran tres ejemplos de servicios diferentes para ayudarlo a entender cómo cambia el alcance de seguridad en función de los servicios que elija:

- Servicios de infraestructura
- Servicios de contenedor
- Servicios sin servidor

Su responsabilidad en materia de seguridad no es estática y cambia según el tipo de arquitectura que seleccione. La arquitectura de nube que elija afecta a su tiempo, esfuerzo y costo.

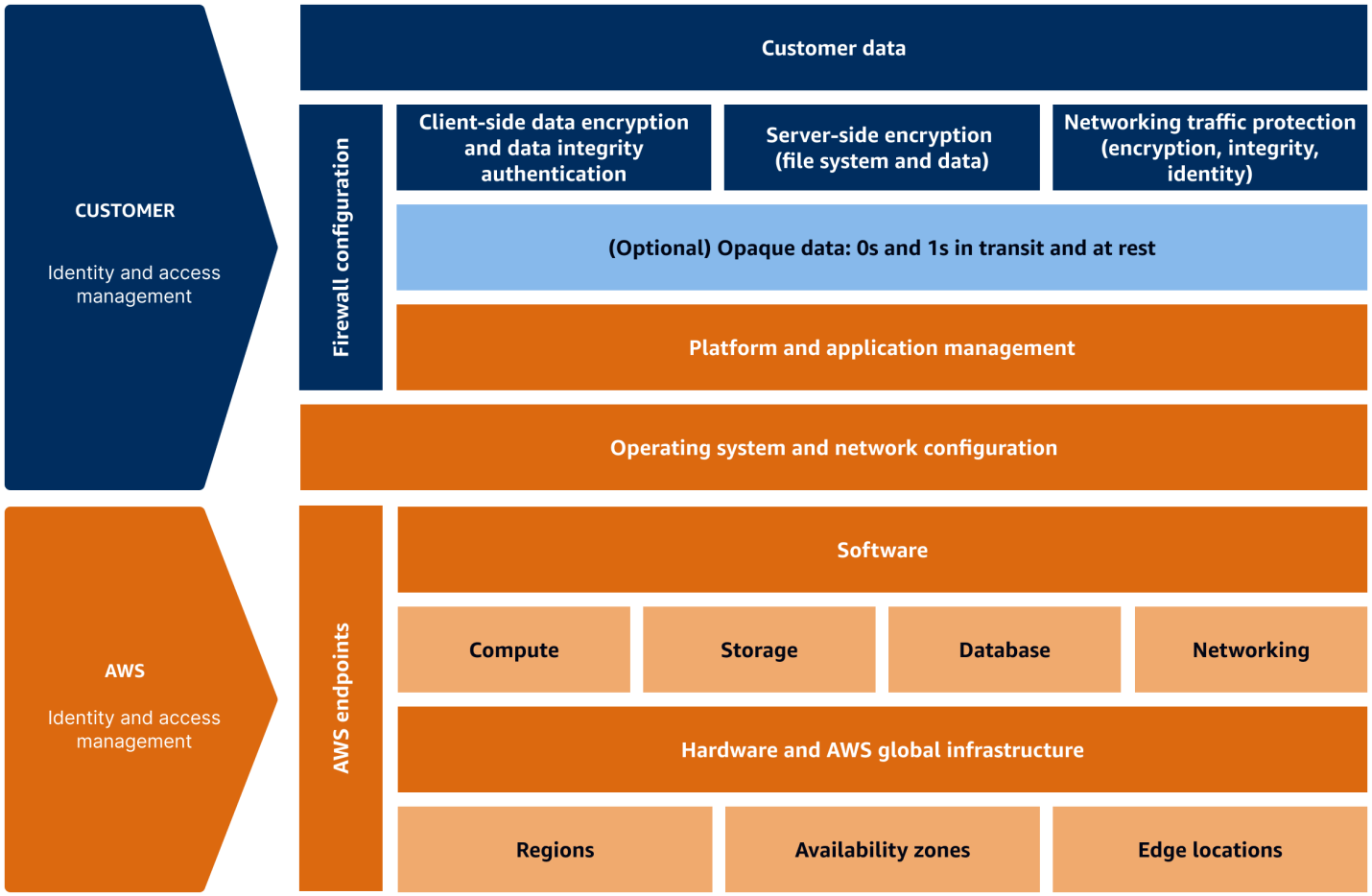
Servicios de infraestructura

En el caso de los servicios de infraestructura, AWS se centra en proteger la infraestructura subyacente. Dentro de los servicios de infraestructura, el alcance es mayor para el cliente porque debe abordar la seguridad de la plataforma, los parches del sistema operativo y la administración de aplicaciones, en comparación con otros modelos. Amazon Elastic Compute Cloud (Amazon EC2) es un ejemplo de servicio de infraestructura común.



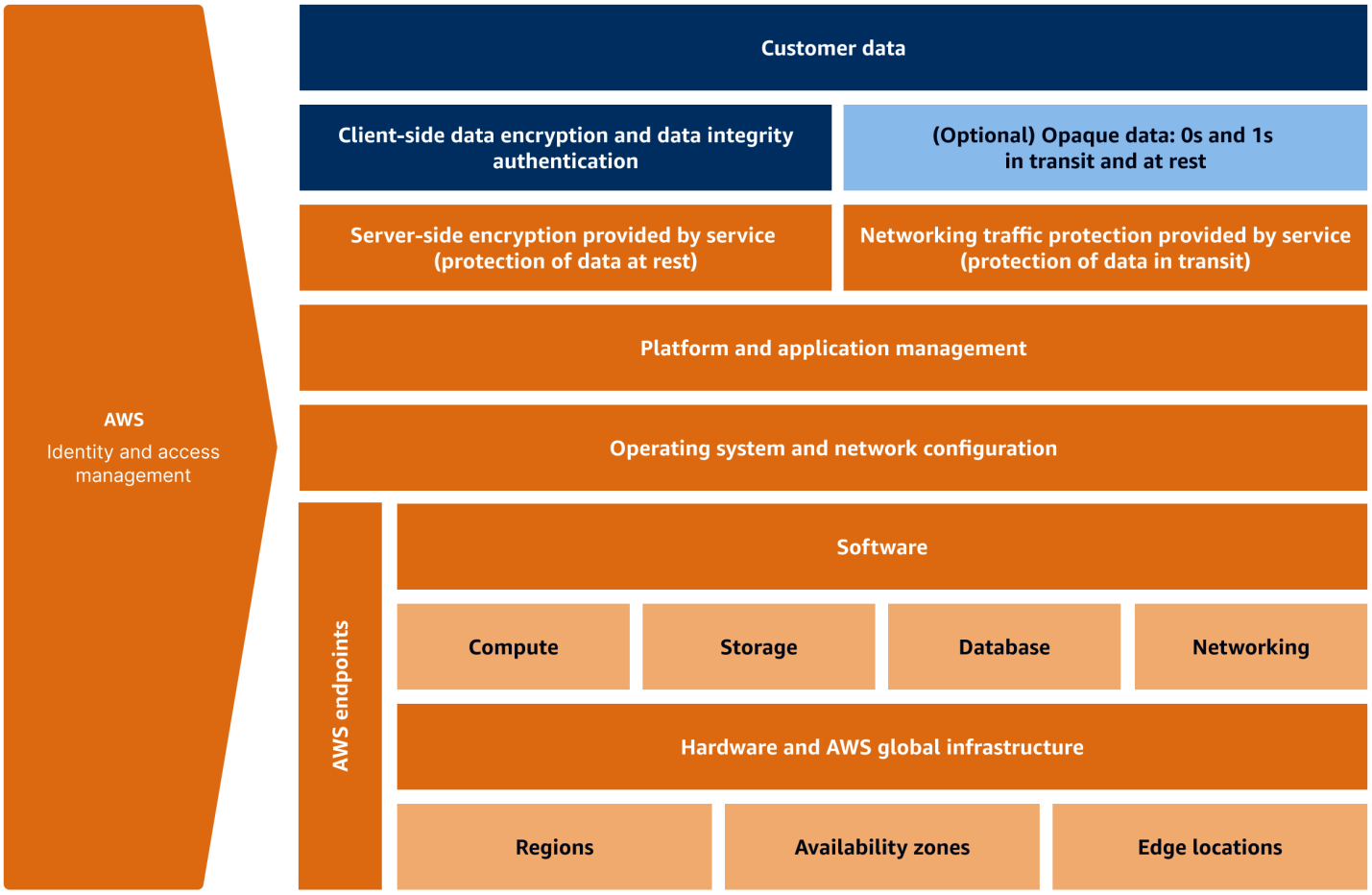
Servicios de contenedor

A medida que la infraestructura se abstrae y moderniza más, la huella se reduce. Su alcance se reduce porque la responsabilidad de algunos elementos de seguridad se traslada a AWS. Los servicios de contenedores son un ejemplo al que se trasladan algunas de las responsabilidades del backend. AWS Por ejemplo, AWS se hace responsable de la configuración del sistema operativo (SO), la configuración de la red, la administración de la plataforma y la administración de las aplicaciones. Algunos ejemplos de servicios de contenedores habituales son Amazon Elastic Kubernetes Service (Amazon EKS), Amazon Elastic Container Registry (Amazon ECR), Amazon Elastic Container Service (Amazon ECS) y AWS Fargate.



Servicios sin servidores

Cuando se utilizan servicios sin servidor, casi toda la responsabilidad de la seguridad recae en nosotros. AWS El alcance de su responsabilidad es mínimo. Por ejemplo, una base de datos sin servidor administrada elimina la necesidad de proteger la red, el hardware y el sistema operativo. AWS cubre todos los parches de sistemas operativos y bases de datos. Su única preocupación es garantizar el acceso a los datos a través del cifrado y la autenticación.



Elección de un modelo de seguridad

Puede elegir entre varios modelos o enfoques de seguridad de AWS. La elección del enfoque y del modelo más adecuado dependen de la audiencia, los objetivos de resultados empresariales y el proceso empresarial general. Es posible utilizar una combinación de varios modelos.

A continuación, se muestran algunos modelos comunes:

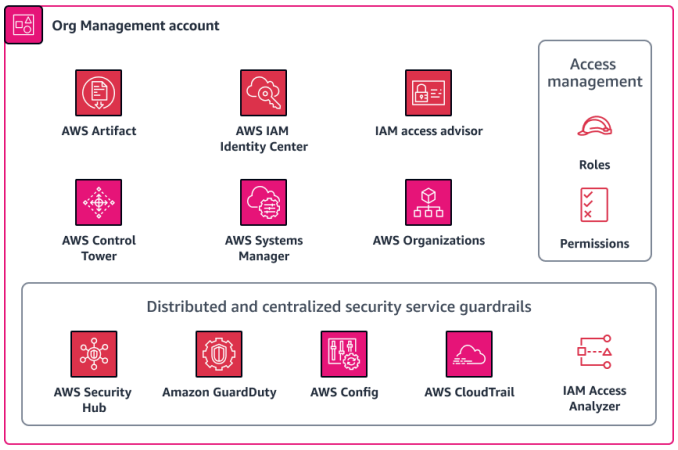
- Modelo de la arquitectura
- Modelo de madurez
- Modelo de gobernanza

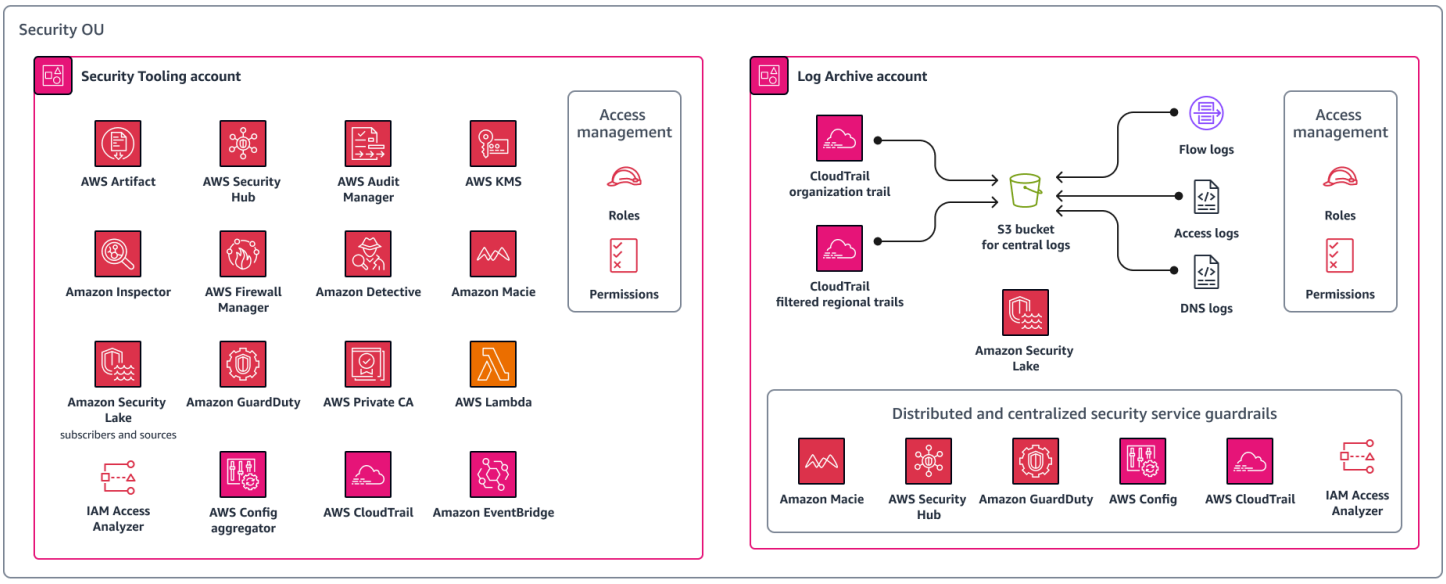
Cada modelo tiene sus propias ventajas y desventajas. Es importante tener en cuenta qué enfoque es el más adecuado para la organización. Implique a los profesionales de la seguridad en las primeras etapas del proceso de modernización de la infraestructura y de adopción de estrategias

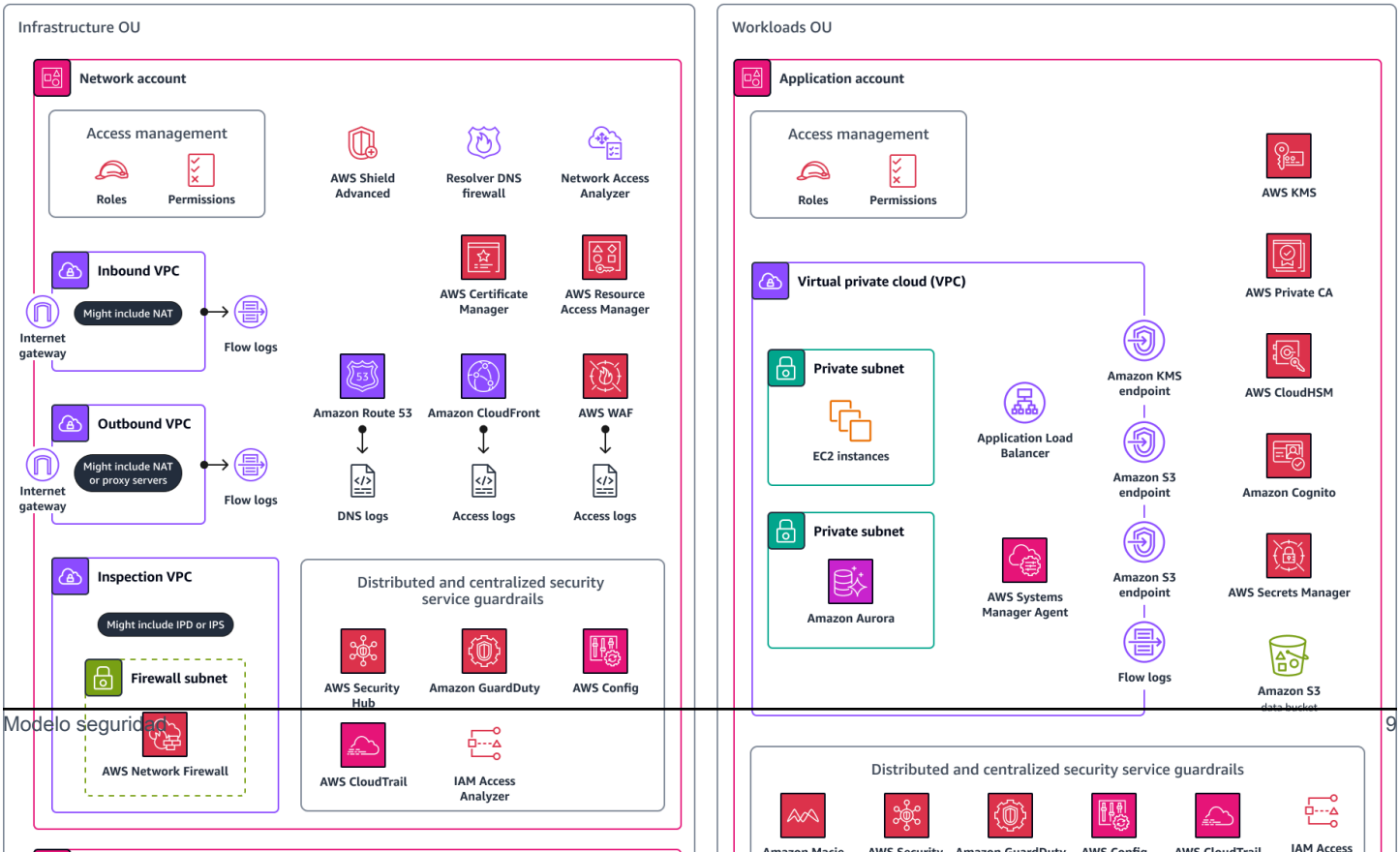
de nube. El modelo que elija tiene un impacto significativo en los roles y las responsabilidades de la organización.

Modelo de la arquitectura

En la siguiente imagen se muestra la Arquitectura de referencia de seguridad de AWS. Este enfoque de arquitectura proporciona un esquema para un modelo de seguridad. Este enfoque es el más adecuado cuando interactúa con los equipos técnicos de la organización. Ayuda a establecer un objetivo futuro ideal. También se alinea con muchos marcos y normas de cumplimiento de AWS .


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
Amazon Security Lake
subscribers and sources
Amazon GuardDuty
AWS Private CA
AWS Lambda
IAM Access Analyzer
AWS Config aggregator
AWS CloudTrail
Amazon EventBridge
Log Archive account
CloudTrail organization trail
CloudTrail filtered regional trails
S3 bucket for central logs
Flow logs
Access logs
DNS logs
Amazon Security Lake
Access management
Roles
Permissions
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer


Infrastructure OU
Network account
Access management
Roles
Permissions
AWS Shield Advanced
Resolver DNS firewall
Network Access Analyzer
AWS Certificate Manager
AWS Resource Access Manager
Inbound VPC
Might include NAT
Internet gateway
Flow logs
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 IPD or IPS
Firewall subnet
AWS Network Firewall
Distributed and centralized security service guardrails
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer
Workloads OU
Application account
Access management
Roles
Permissions
AWS KMS
AWS Private CA
Virtual private cloud (VPC)
Private subnet
EC2 instances
Private subnet
Amazon Aurora
Application Load Balancer
AWS Systems Manager Agent
Amazon KMS endpoint
Amazon S3 endpoint
Amazon S3 endpoint
Flow logs
AWS CloudHSM
Amazon Cognito
AWS Secrets Manager
Amazon S3
Distributed and centralized security service guardrails
Amazon Macie
AWS Security Hub
Amazon GuardDuty
AWS Config
AWS CloudTrail
IAM Access Analyzer

Ventajas del modelo de la arquitectura:

- Cumple con los requisitos de la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA) y del Marco de seguridad común de Health Information Trust Alliance (HITRUST CSF).
- Proporciona una perspectiva de la arquitectura.
- Cumple con las estrategias y directrices de la nube para grandes empresas.
- Se alinea con el marco de adopción de la AWS nube (AWS CAF)
- Cumple con el Marco de AWS Well-Architected.

Desventaja del modelo de la arquitectura:

- Se centra en la tecnología en lugar de la empresa.

Modelo de madurez

El enfoque del modelo de madurez en materia de seguridad de AWS se centra en administrar y reducir el riesgo al priorizar la implementación de las medidas de seguridad. Este enfoque es adecuado para los directores de seguridad CISOs, pero no está centrado en los negocios.

Ventajas del modelo de madurez:

- Se centra en la seguridad.
- Es un modelo que se centra en utilizar un enfoque de implementación ágil.
- Ayuda a reducir el riesgo rápidamente.
- Se alinea con el Marco de Adopción de la AWS Nube (CAF)AWS

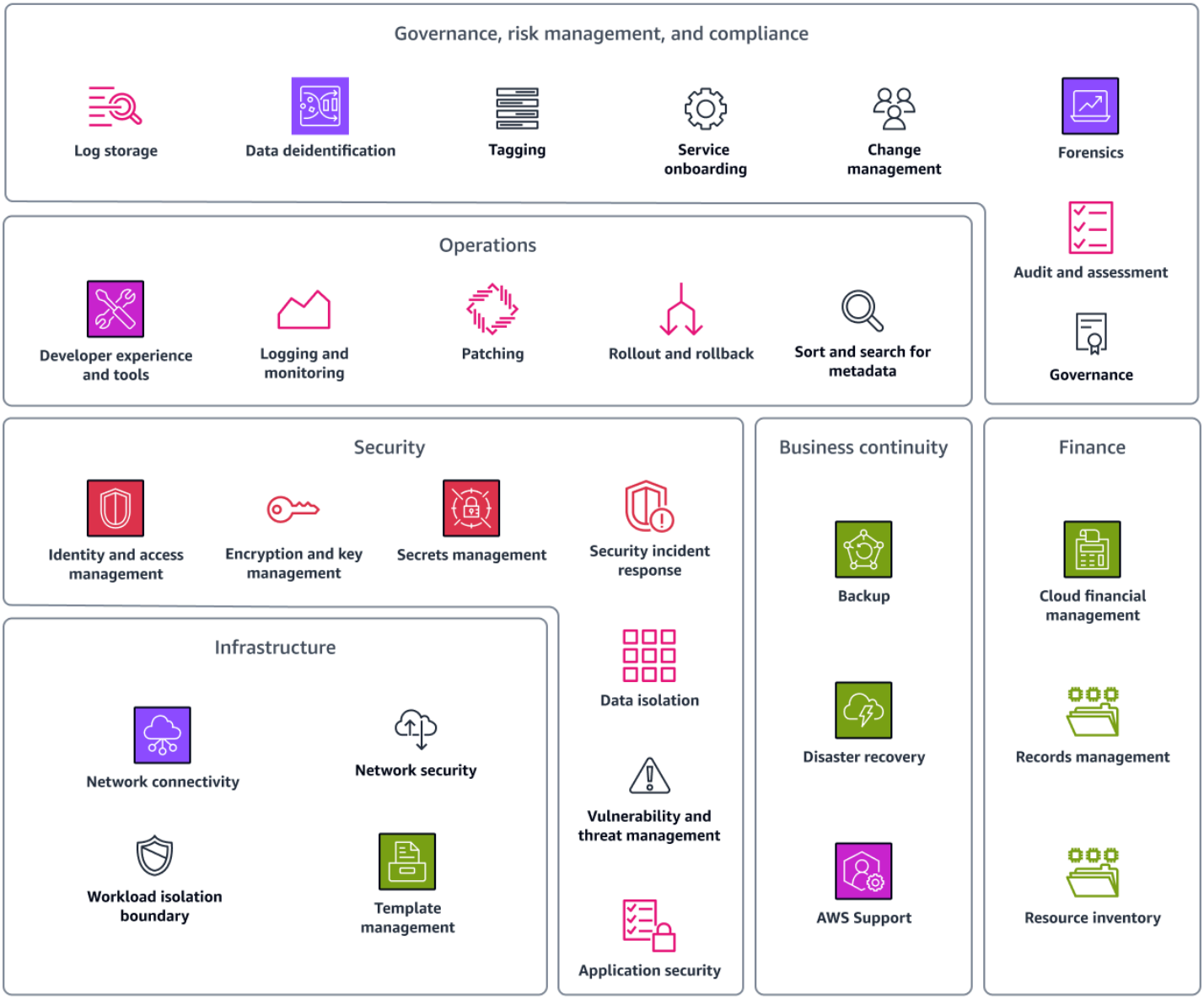
Desventajas del modelo de madurez:

- Se centra en la tecnología en lugar de la empresa.

Modelo de gobernanza

El modelo Fundamentos de la nube en AWS usa un enfoque de gobernanza, administración de riesgos y cumplimiento (GRC) para ayudar a las organizaciones a satisfacer los requisitos de seguridad y cumplimiento. Define las políticas generales que debe seguir el entorno en la nube. Las

capacidades de este modelo lo ayudan a definir los elementos de la acción, definir la propensión al riesgo y alinear las políticas internas.



El modelo Cloud Foundation es una guía de capacidades y gobierno que le ayuda a crear y desarrollar su Nube de AWS entorno. Se basa en un conjunto de definiciones, escenarios, directrices y automatizaciones. La guía incluye los aspectos relacionados con las personas, los procesos y la tecnología relacionados con el establecimiento de un entorno de Nube de AWS . Incluye seis categorías de capacidades que son esenciales para los fundamentos de la nube:

- Gobernanza, administración de riesgos y cumplimiento
- Operaciones

- Seguridad
- Continuidad empresarial
- Finanzas
- Infraestructura

La guía también proporciona ejemplos, plazos y lecturas adicionales para cada capacidad.

Ventajas del modelo de gobernanza:

- Tiene un amplio enfoque tecnológico.
- Está diseñado para ofrecer fiabilidad.
- Utiliza un enfoque operativo.

Desventaja del modelo de gobernanza:

- Se centra en la tecnología en lugar de la empresa.

Creación de un modelo de objetivos empresariales

El modelo de objetivos empresariales implica la definición de los resultados empresariales. Es similar al AWS Cloud Adoption Framework y al AWS Well-Architected Framework. Este enfoque se centra en lo que interesa a la empresa mediante la interpretación de los objetivos de los resultados empresariales. El valor de este enfoque es que es fácil relacionar los objetivos empresariales con los objetivos de seguridad. Un ejemplo de objetivo empresarial es “permitir conexiones externas seguras y el aprovisionamiento acelerado de nuevos usuarios y entornos mediante la automatización de la visibilidad y la comparación con las prácticas recomendadas para reducir el riesgo de forma continua”. Establezca objetivos de tecnología que lo ayuden a alcanzar los resultados empresariales correspondientes. El modelo de objetivos empresariales está relacionado con los objetivos de seguridad, como el mantenimiento de la visibilidad. A continuación, debe implementar un objetivo técnico, como las mejores prácticas de seguridad AWS Identity and Access Management (IAM), para reducir el riesgo de seguridad.

Ventajas del enfoque de objetivos empresariales:

- Incluye la justificación de los costos.
- Proporciona una dirección de seguridad clara y alineada con la empresa.

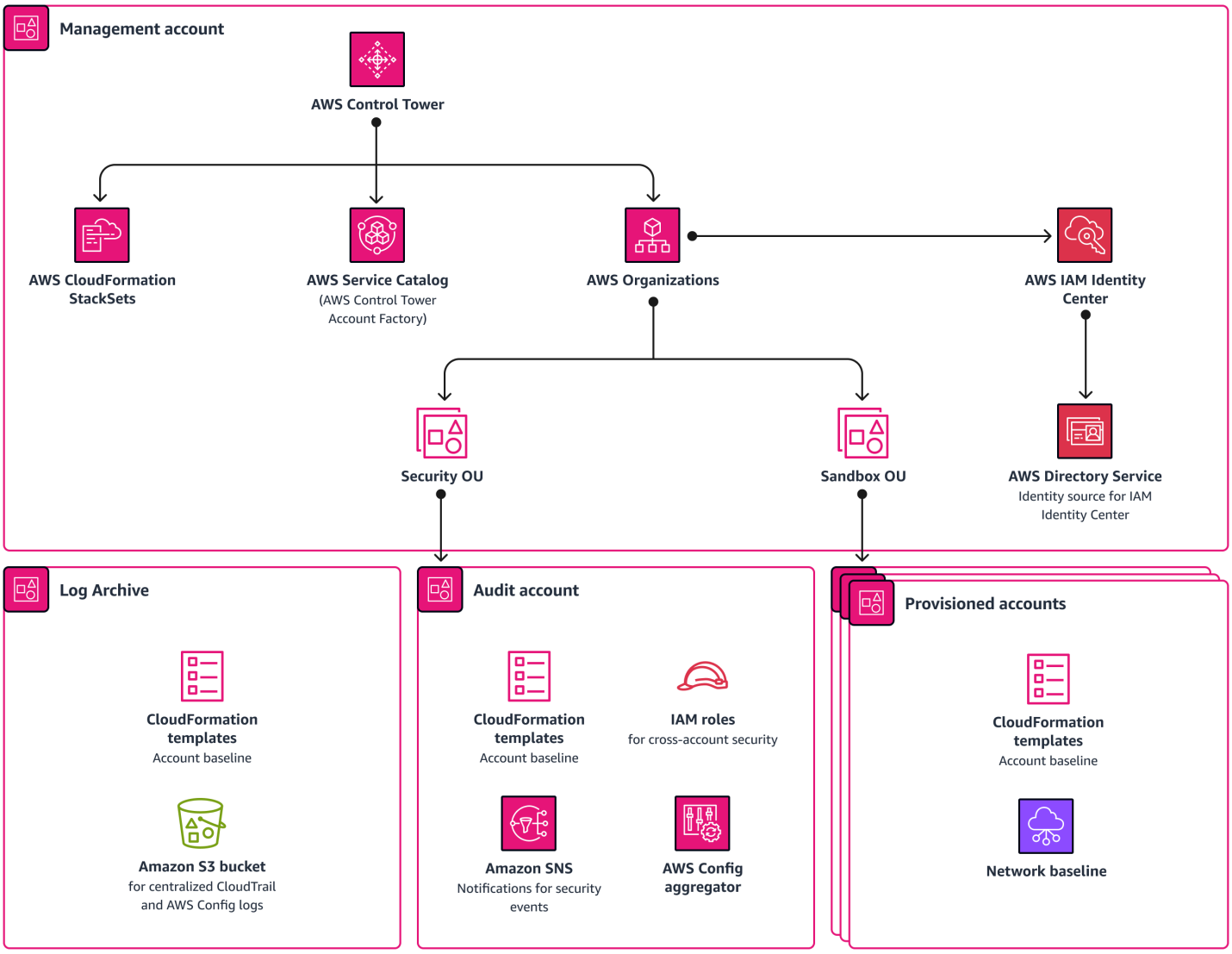
- Define las medidas del éxito mediante el logro de los objetivos de los resultados empresariales.

Desventajas del enfoque de objetivos empresariales:

- Puede llevar mucho tiempo porque hay que averiguar qué quiere la empresa.
- Se centra en la empresa en lugar de la tecnología.

Creación: cómo sentar las bases para unos fundamentos de seguridad de la nube sólidos

Ahora que ya tiene un plan, el siguiente paso es sentar las bases. Este paso demuestra cómo construir una base de nube inicial AWS que sea segura, resiliente, escalable y automatizada en varias cuentas. Puede diseñar y personalizar específicamente cómo sentar las bases de acuerdo con los objetivos empresariales. Puede adaptar los controles a una nueva zona de aterrizaje o incluirlos en una zona de aterrizaje existente. Las automatizaciones de AWS Control Tower pueden ayudarlo a sentar las bases en materia de seguridad en la Nube de AWS. La siguiente imagen muestra una landing zone que se configura a través de ella AWS Control Tower.



AWS Control Tower organiza varios Servicios de AWS en su nombre, como AWS Organizations AWS Service Catalog, y AWS IAM Identity Center. Puede configurar una nueva zona de aterrizaje en una hora, que esté diseñada para satisfacer los requisitos de seguridad y cumplimiento. AWS Control Tower configura la zona de aterrizaje de acuerdo con las prácticas recomendadas de seguridad prescriptivas. AWS Control Tower lo ayuda a administrar el aprovisionamiento en la nube al mejorar la visibilidad y el control sobre las cuentas y los usuarios finales. Ayuda a los administradores a asignar y supervisar de forma eficiente los recursos de computación, implementar un control de acceso basado en roles, supervisar el rendimiento mediante herramientas de registro y supervisión, administrar los costos de forma eficaz, automatizar los procesos de implementación, aplicar las medidas de seguridad y garantizar el cumplimiento de los estándares del sector.

AWS Control Tower es la forma más rápida de configurar y administrar un AWS entorno multicuenta seguro, que cumpla con las normas y se base en las mejores prácticas. Para obtener más información sobre cómo trabajar con la estrategia AWS multicuenta AWS Control Tower y las prácticas recomendadas que se describen en ella, consulte la guía sobre estrategias AWS multicuentas: prácticas recomendadas.

Aunque AWS Control Tower es el enfoque más rápido, no es el único. Lo importante es que establezca una zona de aterrizaje que, como mínimo, proporcione lo siguiente:

- Administración multicuenta
- Administración de accesos federados e identidades
- Un archivo centralizado para los registros
- Acceso de auditoría entre cuentas
- Aprovisionamiento de cuentas de usuarios finales
- Supervisión y notificaciones centralizadas

Evaluación: evaluación de la posición de seguridad en la nube actual

Antes de implementar nada en la zona de aterrizaje, evalúela para asegurarse de que cumpla con los requisitos y establecer una línea de base. Esta práctica se conoce como evaluación de la posición en la nube. Lo ayuda a identificar y corregir los riesgos en toda la infraestructura en la nube. La evaluación de la posición de seguridad en la nube proporciona visibilidad de los controles de seguridad pertinentes en el entorno de nube.

A continuación se indican los beneficios de evaluar la posición en la nube:

- Lo ayuda a comprender la posición de seguridad actual y obtener recomendaciones para reducir el perfil de riesgo, corregir las vulnerabilidades existentes o corregir los errores de configuración.
- Lo ayuda a identificar las prácticas recomendadas de seguridad para evitar errores y reducir los riesgos empresariales.
- Proporciona métricas que lo ayudan a hacer un seguimiento de las mejoras y medir el éxito.

En esta sección, se analizan los servicios AWS Security Hub CSPM y Prowler las herramientas que puede utilizar para realizar una evaluación del estado de su entorno frente a la nube.

Prowler

Prowleres una herramienta de línea de comandos de código abierto que le ayuda a evaluar, auditar y supervisar sus cuentas para comprobar si cumplen las mejores prácticas de AWS seguridad y otros marcos y estándares de seguridad. Inspecciona la configuración e identifica los problemas de seguridad. Puede utilizarla Prowler en entornos con varias cuentas, y los proveedores externos también pueden utilizarla para evaluar la seguridad de su entorno. AWS

A continuación se describen los beneficios de Prowler:

- Es gratuito y de código abierto.
- Cuenta con opciones de implementación flexibles y es escalable.
- Realiza comprobaciones de conformidad, como las de referencia del Center for Internet Security (CIS) AWS, el Reglamento General de Protección de Datos (GDPR) y la HIPAA.
- Lo ayuda a crear instantáneas y líneas de base.

AWS Security Hub CSPM

AWS Security Hub CSPMproporciona una visión completa de su estado de seguridad en. AWS También le permite comprobar si su entorno de cumple con los estándares y las prácticas recomendadas del sector de seguridad. Está integrado AWS Control Tower para que pueda configurar los controles de detección del Security Hub CSPM a través del AWS Control Tower servicio. El objetivo de acelerar la madurez de la seguridad consiste en hacer que el proceso de evaluación pase de ser una instantánea única a convertirse en un proceso continuo de supervisión del progreso.

Las siguientes son las ventajas de Security Hub CSPM:

- Proporciona un panel unificado que muestra el estado actual del entorno y lo ayuda a identificar y solucionar los problemas.
- Lleva a cabo evaluaciones continuas con comprobaciones automatizadas.

Etapa de caminar: operación y madurez

La etapa de caminar se centra en la operación. Durante esta etapa, la organización debe evaluar el modelo operativo actual, determinar cómo debe adaptarse a la nube, implementar esos cambios y, a continuación, medir el progreso. Esto incluye abordar las habilidades, los procesos operativos y la tecnología. Ajustar la implementación de la nube y medir el progreso es fundamental durante toda la etapa para validar el éxito.

A continuación se muestran las fases de la etapa de caminar:

- Operación: ¿cómo prepara al personal, la tecnología y los procesos para la nube?
- Madurez: ¿cómo se miden el progreso y el éxito?

Operación: preparación de la organización para una posición de seguridad de nube madura

Para avanzar en el proceso de implementación de las cargas operativas en la nube, es importante centrarse en la alineación de las personas, los procesos y la tecnología. Es particularmente crucial en el entorno en la nube, ya que es probable que los procesos y las habilidades difieran de los de las operaciones en las instalaciones. En esta sección, utilizará un marco para alinear al personal, los procesos y la tecnología y, a continuación, confirmará que el marco lo haya ayudado a lograr los resultados esperados.

AWS Marco de adopción de la nube

El marco de adopción de la AWS nube (AWS CAF) lo ayuda a acelerar los resultados de su negocio mediante el uso Servicios de AWS y las funciones innovadores. AWS CAF identifica seis perspectivas organizativas específicas que sustentan las transformaciones exitosas de la nube: negocios, personas, gobierno, plataforma, seguridad y operaciones. Cada perspectiva contiene

capacidades que pueden mejorar la preparación para la nube y ayudarlo a acelerar su proceso de transformación de nube.

La siguiente imagen muestra las seis perspectivas de la AWS CAF y las capacidades de cada perspectiva. Para más información, consulte Capacidades fundamentales en Información general sobre AWS Cloud Adoption Framework.

Resultados esperados

Cuando utiliza la AWS CAF para alinear a su personal, sus procesos y su tecnología, puede esperar lograr los siguientes resultados:

- DevSecOps Canalización y proceso: la implementación de una DevOps canalización con herramientas de seguridad integradas puede ayudarle a implementar la infraestructura como código (IaC) de forma más segura. Puede implementar el escaneo del código y las comprobaciones de seguridad en el proceso de procesamiento, como cfn_nag (GitHub), que es un analizador de código estático de código abierto.
- Etiquetado y gestión de activos: las etiquetas pueden ayudarlo a administrar los recursos en la nube de forma más eficiente y coherente. Para obtener más información, consulte Etiquetado de los recursos de AWS. Es importante desarrollar una estrategia de gestión de activos dinámica que pueda adaptarse a la naturaleza de la nube, en constante cambio. El AWS Systems Manager inventario lo ayuda a asignar etiquetas para que pueda buscar, administrar e identificar los recursos rápidamente.
- Integración de la supervisión y la detección: es fundamental establecer un método para enviar alertas desde la nube a los centros de operaciones de seguridad locales (SOCs) y a los sistemas de información de seguridad y gestión de eventos (SIEM). Amazon GuardDuty es un servicio de supervisión continua de la seguridad que analiza y procesa los registros para identificar actividades inesperadas y potencialmente no autorizadas en su AWS entorno. También se integra con muchas herramientas de terceros.
- Planificación y programación de respuesta ante incidentes en la nube: es importante asegurarse de que el personal responsable de gestionar las alertas en la nube esté familiarizado con el proceso de ingesta de las alertas y sepa cómo responder ante alertas en la nube, en comparación con las alertas en las instalaciones. Para mejorar las capacidades de respuesta ante incidentes, forme al personal para que utilice Amazon Detective para el análisis de registros. Amazon Detective lo ayuda a analizar, investigar e identificar la causa raíz de resultados de seguridad o actividades sospechosas. Amazon Detective debe formar parte de un plan de respuesta ante incidentes.
- Administración de vulnerabilidades en la nube: el proceso de administración de las vulnerabilidades en la nube es diferente al de los entornos en las instalaciones. Además de la administración de vulnerabilidades tradicional, también debe evaluar la capa de código de la infraestructura. Amazon Inspector es un servicio de administración de vulnerabilidades automatizadas que evalúa de forma continua los recursos en busca de vulnerabilidades y exposición de la red no deseada.

- Administración de la posición en la nube: la administración de la posición en la nube, tal como se describe en la sección Evaluación, es un aspecto importante de la seguridad en la nube. Puede utilizarlo AWS Security Hub CSPM para automatizar las comprobaciones de las mejores prácticas de seguridad y evaluar su postura general en relación con la nube en todos sus ámbitos Cuentas de AWS.
- Formación en seguridad de nube: es esencial proporcionar la formación adecuada a los empleados para que dominen la seguridad de nube. Esto incluye proporcionar acceso a los recursos y asignar tiempo a los empleados para que adquieran los conocimientos y las habilidades necesarios. AWS proporciona muchos recursos de formación para mejorar sus habilidades y educar, como AWS Skill Builder.

Madurez: ajuste y medición de los procesos, las herramientas y el riesgo

En la fase madura del modelo de seguridad en la nube, la atención se centra en alinear los equipos de seguridad con las capacidades de seguridad del AWS Cloud Adoption Framework (AWS CAF) y en instituir procesos ágiles. Esta alineación ayuda a los equipos especializados a acelerar la innovación en periodos cortos y, al mismo tiempo, incorpora hojas de ruta y una planificación a largo plazo. La fase de madurez remarca la colaboración con las operaciones de TI y en la adquisición de habilidades en la nube profundas y especializadas. Cada capacidad de seguridad implementa herramientas y procesos clave para mejorar la eficiencia y el impacto, además del desarrollo de métricas y mecanismos de informes para medir los cambios incrementales y el impacto general.

En esta etapa, hará lo siguiente:

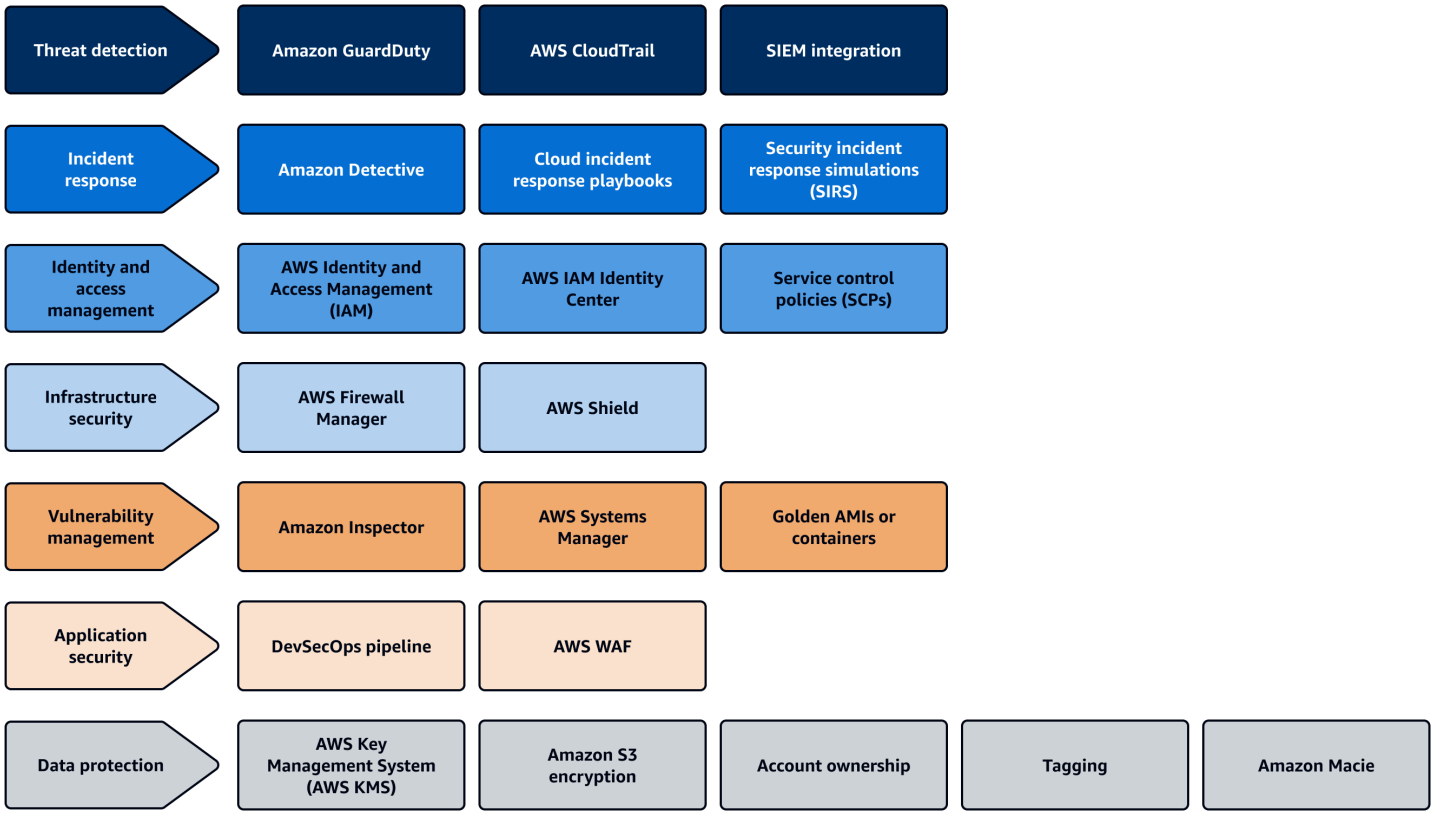
- Ajuste y medición de procesos
- Ajuste y medición de las herramientas
- Ajuste y medición del riesgo
- Consulta de ejemplos de casos de uso en la fase de madurez

Ajuste y medición de procesos

El enfoque ágil proporciona más flexibilidad e innovación, y puede ayudarlo a probar e implementar nuevas ideas rápidamente. Divida sus equipos de seguridad en roles especializados, como personal de respuesta ante incidentes y administradores de vulnerabilidades. Las funciones deben alinearse

con las categorías de la siguiente imagen, que corresponden a las capacidades del Marco de adopción de la AWS nube (AWS CAF). El enfoque ágil anima a los equipos a pensar en grande, inventar, simplificar e identificar posibles deficiencias en materia de seguridad. Esto da como resultado la creación de historias de usuarios o hojas de ruta pendientes para futuras mejoras.

Un proceso ágil permite soluciones más dinámicas y adaptables, en lugar de depender solo de las capacidades de una herramienta específica. Responder rápido a los errores es una filosofía que utiliza pruebas frecuentes e incrementales para reducir el ciclo de vida del desarrollo y es una parte fundamental de un enfoque ágil. Haga un cambio, pruébelo y, a continuación, decida si desea continuar con el enfoque actual o cambiar a uno alternativo. Si los equipos trabajan en este ciclo, ayudan a su organización a mantenerse al día con la naturaleza acelerada de la nube. La formación específica también es fundamental: debe ofrecer una formación específica para un dominio concreto de la seguridad de la nube.



> **Note**
>
> Esta imagen no contiene las capacidades de garantía y gobierno de la seguridad de la AWS CAF. Esta guía se centra en las operaciones de seguridad, y la garantía y gobernanza de seguridad quedan fuera del ámbito de esta guía. Para obtener más información sobre la

garantía de seguridad, consulte AWS Re:inForce 2023: Scaling compliance with on. AWS Control Tower YouTube

En la organización, utilice un enfoque ágil que la ayude a mantenerse al día con el rápido desarrollo y los cambios en la nube. A continuación se muestran algunas formas de comenzar a experimentar e iterar en su entorno de nube:

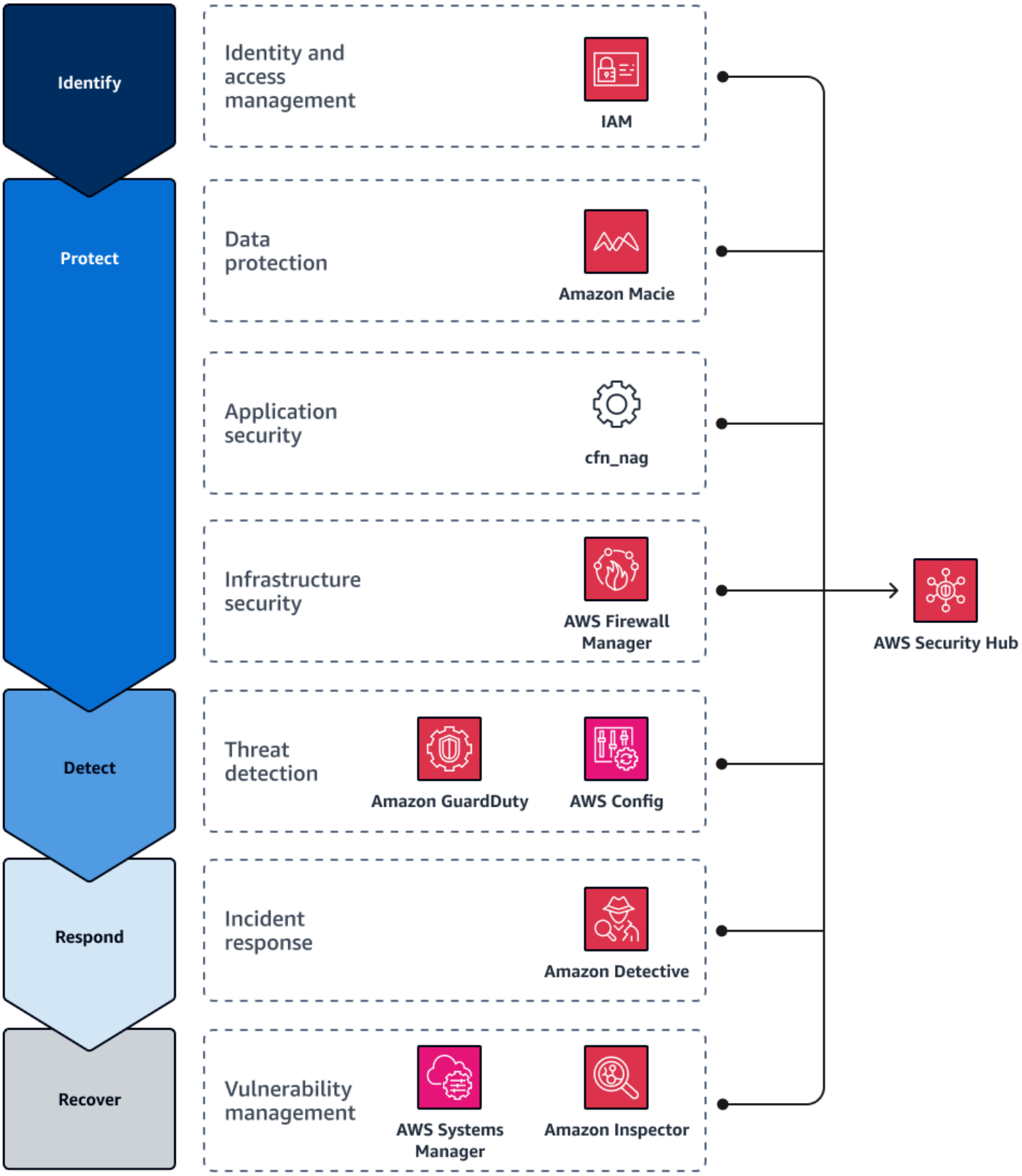
- Especialícese en las categorías definidas en AWS CAF, como se muestra en la imagen anterior.
- Por cuestiones de dinamismo, céntrese en la innovación en lugar de en las operaciones.
- Avance con rapidez en sprints al permitir que las personas hagan pruebas, respondan rápido a los errores e implementen rápidamente, y continúe con este ciclo para mantenerse al día con el negocio.
- Para respaldar las operaciones continuas, siempre que sea posible, alinee los procesos para los entornos en las instalaciones y basados en la nube.
- Para ayudar a las personas a profundizar y centrarse en un área, ofrezca una formación específica en lugar de amplia.
- Anime a las personas a pensar en grande, investigar “qué pasaría si” y crear tareas pendientes (como hojas de ruta o deficiencias).

Ajuste y medición de las herramientas

Después de establecer equipos especializados para diferentes dominios de seguridad, alinéelos entre sí. AWS Security Hub CSPM puede ayudarlo a lograrlo. Security Hub CSPM proporciona un panel de control centralizado y unificado para monitorear el progreso en comparación con los marcos. También se integra con los servicios AWS de seguridad muchas herramientas de terceros.

El Marco de ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST), que figura en el sitio web del NIST, consta de cinco funciones: identificar, proteger, detectar, responder y recuperar. La siguiente imagen muestra cómo puede utilizar diferentes Servicios de AWS durante cada función y, a continuación, configurar esos servicios para que envíen sus conclusiones al Security Hub CSPM para la elaboración de informes consolidados. Si opta por utilizar otras herramientas, puede utilizar la API CSPM de Security Hub, AWS Command Line Interface (AWS CLI) y el AWS Security Finding Format (ASFF) para crear integraciones personalizadas. Para obtener más información sobre las integraciones de CSPM de Security Hub con otros servicios, consulte

Integraciones de productos en la documentación de CSPM AWS Security Hub CSPM de Security Hub.



Security Hub CSPM se integra con todos estos servicios y herramientas y proporciona lo siguiente:

- Proporciona un panel unificado que muestra las actualizaciones y ayuda a los equipos a iterar in situ.
- Se integra automáticamente con servicios de AWS seguridad, como Amazon Macie GuardDuty, Amazon yAmazon Detective
- Admite la integración con herramientas de terceros, como Prowler y cfn_nag.
- Admite integraciones personalizadas con herramientas, como la API CSPM de Security Hub y el AWS Security Finding Format (ASFF) AWS CLI

Ajuste y medición del riesgo

Durante la fase madura de la etapa de caminata, puede utilizarla AWS Security Hub CSPM para ajustar y medir continuamente el riesgo de seguridad. Security Hub CSPM evalúa continuamente la postura de seguridad de una organización y toma medidas para solucionar los problemas identificados. Security Hub CSPM centraliza y prioriza los hallazgos de seguridad de todos los servicios y Cuentas de AWS socios externos compatibles. Esto ayuda a analizar las tendencias de seguridad e identificar los problemas de seguridad de alta prioridad.

Security Hub CSPM realiza cientos de comprobaciones de seguridad y las clasifica en función del riesgo para su entorno. AWS Puedes ver tu puntuación comparándola con los controles de seguridad en un panel unificado en la consola CSPM de Security Hub. Para obtener más información, consulte Determinación de los puntajes de seguridad en la documentación de CSPM de Security Hub. A través de este panel, la DevSecOps función puede identificar rápidamente cualquier comprobación que haya fallado, la gravedad del problema de seguridad Región de AWS y qué recurso está afectado. Una vez identificado, el DevSecOps equipo puede priorizar y solucionar el problema. A medida que se solucionan los problemas, Security Hub CSPM actualiza automáticamente el estado.

Consulta de ejemplos de casos de uso en la fase de madurez

A continuación se muestran ejemplos de la fase de madurez. En estos ejemplos se profundiza en los modelos, las herramientas y los procesos para los diferentes objetivos empresariales de forma práctica.

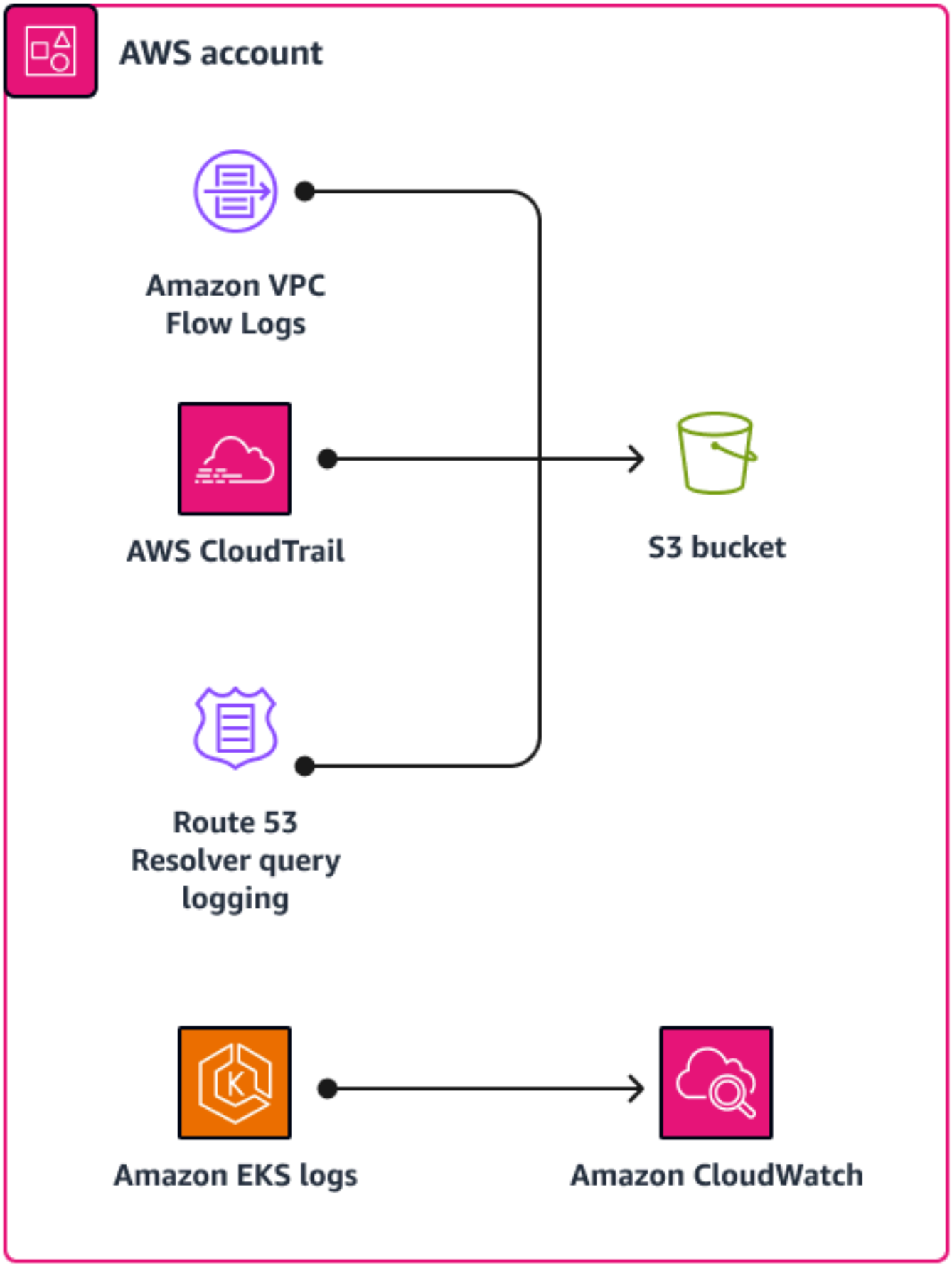
Madurez: ejemplo de detección de amenazas

Resultado empresarial de los controles de detección: aumente la visibilidad y la velocidad de detección de los incidentes en la nube para reducir el riesgo y permitir el uso y el desarrollo acelerados de los recursos de nube.

Herramienta: el Assisted Log Enabler for AWS (GitHub) es una herramienta de código abierto que lo ayuda a activar el registro durante un incidente de seguridad. Puede aumentar rápidamente la visibilidad de un incidente.

Ejemplo de caso de uso: considere el caso de uso de una sola cuenta que se muestra en el siguiente diagrama. Hay eventos que requieren una investigación más profunda. No sabe con certeza si el registro está activado. En este caso, lo mejor es realizar una prueba con el Assisted Log Enabler para ver qué servicios están habilitados o deshabilitados. Assisted Log Enablercomprueba las AWS CloudTrail rutas, los registros de consultas de DNS, los registros de flujo de VPC y otros registros. Si no están habilitados, los Assisted Log Enabler habilita. Assisted Log Enablerpuede comprobar y activar el registro en todas partes Regiones de AWS.

También puede aumentar o reducir la limitación del Assisted Log Enabler. Tras completar la ejecución de pruebas, cerrar el evento y resolver el problema, se da cuenta de que ya no necesita este nivel de registro. Puede limpiar rápidamente la implementación para detener el registro. Esta característica le permite utilizar el Assisted Log Enabler como herramienta de clasificación.


AWS account
Amazon VPC Flow Logs
AWS CloudTrail
S3 bucket
Route 53 Resolver query logging
Amazon EKS logs
Amazon CloudWatch

Estas son algunas de las características principales del Assisted Log Enabler for AWS:

- Puede ejecutarlo en un entorno de una cuenta o multicuenta.
- Puede usarlo para establecer una línea de base para iniciar sesión en el entorno.
- Puede usar la característica de ejecución de pruebas para comprobar el estado actual y determinar qué servicios tienen activado el registro.
- Puede seleccionar los servicios para los que desea habilitar el registro.
- Puede aumentar o reducir la limitación del Assisted Log Enabler para su caso de uso.

Madurez: ejemplo de IAM

Resultado empresarial de IAM: automatice la visibilidad y compárelo con las prácticas recomendadas para reducir el riesgo de forma continua, permitir conexiones externas seguras y aprovisionar rápidamente nuevos usuarios y entornos.

Herramienta: el AWS Identity and Access Management Access Analyzer (Analizador de acceso de IAM) lo ayuda a identificar recursos compartidos con una entidad externa, valida las políticas de IAM con las prácticas recomendadas y la gramática de la política y genera políticas de IAM en función del historial de la actividad de acceso. Le recomendamos encarecidamente que habilite el Analizador de acceso de IAM tanto en la cuenta como en la organización.

Beneficios del servicio: el Analizador de acceso de IAM ofrece una gran cantidad de resultados reveladores. Puede ayudarlo a identificar los recursos de la organización y las cuentas que se comparten con una entidad externa. Puede detectar recursos como un bucket de S3 público, uno AWS KMS key compartido con otra cuenta o un rol compartido con una cuenta externa, lo que le brinda una excelente visibilidad para identificar los recursos que no están bajo el control de su organización. No solo valida las políticas de IAM, sino que también puede generarlas.

Etapa de correr: optimización de las operaciones de seguridad en la nube

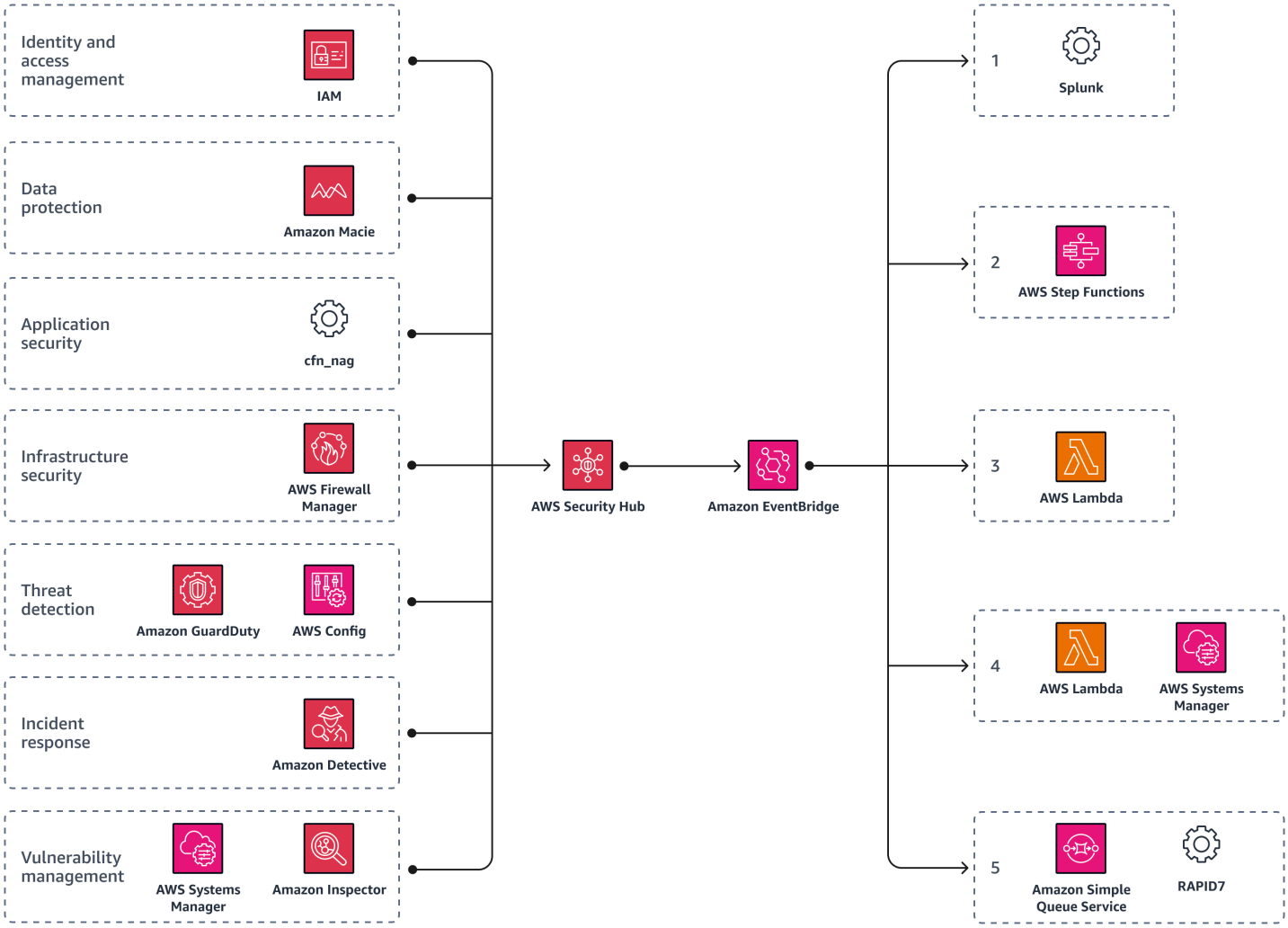
Tras implementar una línea de base en la etapa de caminar, la organización pasa a la etapa de correr. Esta etapa se centra en demostrar las capacidades de ciberseguridad disponibles en la nube, muchas de las cuales no son posibles o son muy difíciles de implementar con soluciones en las instalaciones. En esta etapa se reúnen diferentes componentes de seguridad y se automatizan los procesos. Las automatizaciones liberan los recursos para que puedan centrarse en tareas de alto valor.

A continuación se indica la única fase de la etapa de correr:

- Optimizar: ¿cómo puedo mejorar este proceso y agregar automatización?

Optimización: automatización e iteración de las operaciones de seguridad de nube

En la fase de optimización, automatizará las operaciones de seguridad. Al igual que las etapas de caminar y caminar, puedes utilizarlas AWS Security Hub CSPM durante la etapa de ejecución para lograr la automatización y la iteración. La siguiente imagen muestra cómo Security Hub CSPM puede activar una EventBridge regla de Amazon personalizada que defina las acciones automáticas que se deben tomar en función de hallazgos e información específicos. Para obtener más información, consulte Automatizaciones en la documentación de CSPM de Security Hub.



Al utilizar Security Hub CSPM como centro de automatización central, también puede reenviar actividades a. Splunk Splunkpuede entonces detectar las que son anómalas y activar las acciones correspondientes. EventBridge Esto lo ayuda a automatizar las tareas repetitivas y proporciona más tiempo para que los miembros cualificados del equipo se centren en actividades de mayor valor. También puede utilizar AWS Step Functions para recopilar registros, tomar instantáneas forenses, poner en cuarentena los servidores comprometidos y sustituirlos por una imagen dorada. Además, puede utilizar una función de AWS Lambda que utiliza AWS Systems Manager para corregir vulnerabilidades en todo el entorno y utiliza una función de Amazon Simple Queue Service (Amazon SQS) para validar la seguridad de los sistemas. Al adoptar este enfoque, es posible contener y corregir rápidamente los incidentes de seguridad con un impacto mínimo en las operaciones empresariales habituales.

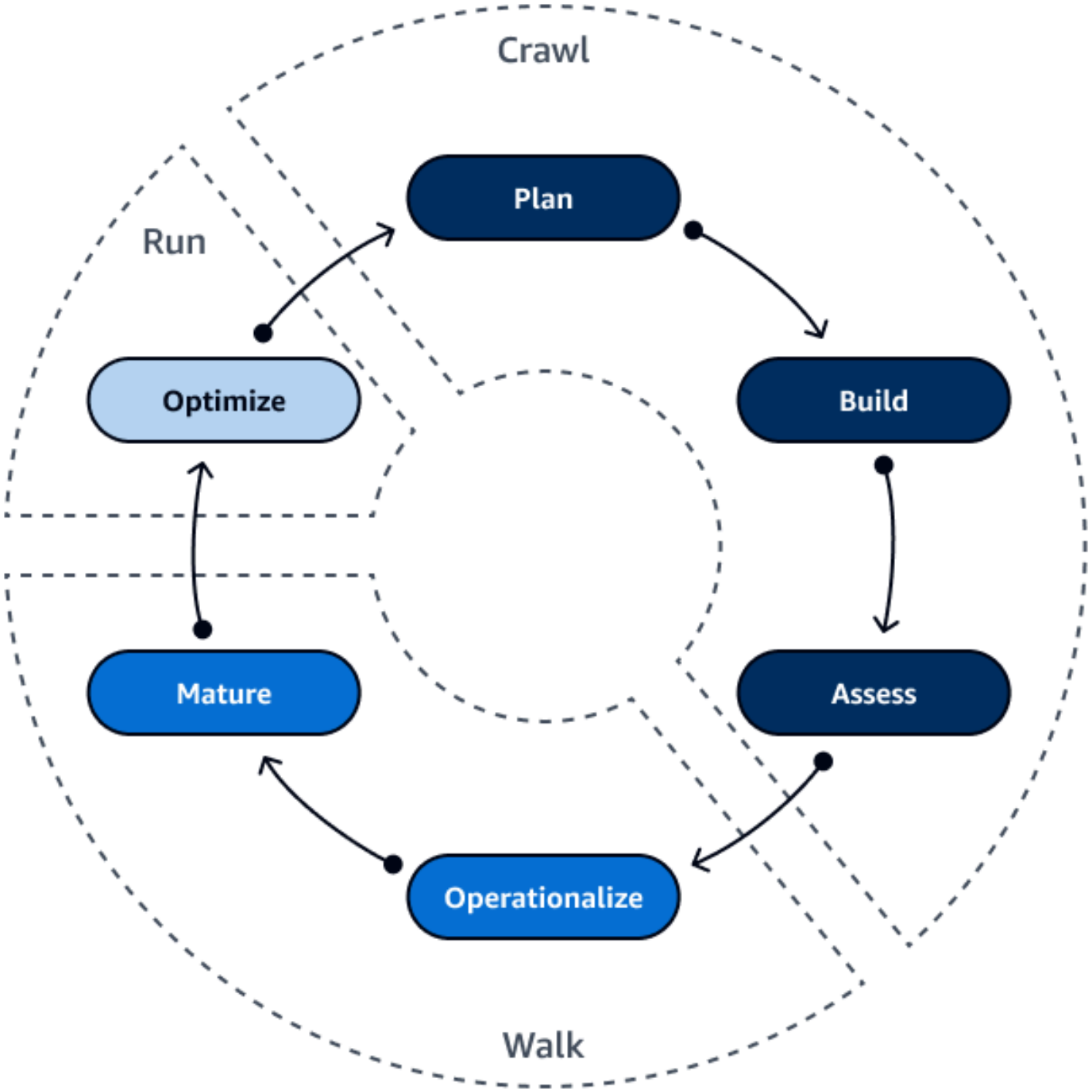
A continuación se muestra un ejemplo de acciones automatizadas repetidas, como se muestra en la imagen anterior:

1. Utilice Splunk para detectar actividades cuestionables.
2. Utilice Step Functions para recopilar registros, revocar el acceso, poner en cuarentena y tomar instantáneas forenses.
3. Utilice una EventBridge regla para iniciar una función Lambda que ponga en cuarentena, tome instantáneas forenses y sustituya los servidores comprometidos por una imagen dorada.
4. Inicie una función de Lambda que utilice Systems Manager para corregir y aplicar parches en el resto del entorno.
5. Inicie un mensaje de Amazon SQS que utilice el escáner Rapid7 para escanear y validar si el AWS recurso es seguro.

Para obtener más información, consulte Cómo automatizar la respuesta a incidentes en las instancias Nube de AWS de EC2 en el AWS blog de seguridad.

Conclusión: ¡gatee, camine, corra y vuele!

En resumen, el modelo gatear, caminar y correr es un marco que lo ayuda a mejorar gradualmente su posición de seguridad y adoptar las prácticas recomendadas para proteger la infraestructura de AWS. Este proceso continúa evolucionando a medida que surgen nuevas tecnologías y necesidades empresariales. Si sigue este marco y utiliza los recursos que ofrece AWS, puede establecer una base sólida para la seguridad en la nube, administrar eficazmente los riesgos de seguridad, acelerar la madurez en materia de seguridad e impulsar la innovación.



En la etapa de gatear, sienta las bases. Defina cuál es el plan de seguridad, utilice una arquitectura de prácticas recomendadas de seguridad definida e impulse una evaluación continua de los objetivos empresariales de la organización.

En la etapa de caminar, da los primeros pasos. Analice las políticas, elabore manuales de estrategias, forme a personas y alinee estrategias. Esta etapa lo ayuda a entender cómo aprovechar la innovación para mantenerse al día con las tecnologías de la nube.

En la fase de correr, piensa en grande. Utilice la automatización y coloque estratégicamente al personal cualificado en el lugar correcto. Implemente la automatización para impulsar la evaluación continua a fin de cumplir los objetivos empresariales de la organización.

Luego, es el momento de volar. Utilice las recomendaciones de esta guía para acelerar la madurez en materia de seguridad en la Nube de AWS.

Recursos

Marcos y modelos

- AWS Cloud Adoption Framework (AWS CAF)
- AWS Well-Architected Framework
- Arquitectura de referencia de seguridad de AWSAWS (SRA de)
- AWS Security Maturity Model
- Arquitectura de referencia de HIPAA
- Arquitectura de referencia de HITRUST

Servicios de AWS

- AWS Control Tower
- AWS Identity and Access Management Access Analyzer
- AWS Security Hub CSPM

Otros recursos de AWS

- Automated Security Response on AWS en la Biblioteca de soluciones de AWS
- Automate Your IT Operations Using AWS Step Functions and Amazon CloudWatch Events en el blog de computación de AWS
- How to automate incident response in the Nube de AWS for EC2 instances en el blog de seguridad de AWS
- How to perform automated incident response in a multi-account environment en el blog de seguridad de AWS
- Video AWS re:Inforce 2022 - Crawl, walk, run: Accelerating security maturity en YouTube
- Presentación en PowerPoint AWS re:Inforce 2022 - Crawl, walk, run: Accelerating security maturity (archivo adjunto)

Colaboradores

Las siguientes personas y organizaciones han colaborado en esta guía.

Creación

- Chad Lorenc, director de prácticas de seguridad, AWS
- Ivy Gin, consultora de garantía de seguridad, AWS
- Sayali Paseband, consultora de seguridad, AWS

Revisión

- Deeps Baisya, arquitecto de seguridad sénior, AWS
- Mike LaRue, consultor de seguridad sénior, AWS
- Raul Radu, ingeniero de seguridad sénior, AWS

Redacción técnica

- Lilly AbouHarb, redactora técnica sénior, AWS

Historial de documentos

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

Cambio	Descripción	Fecha
Publicación inicial	—	20 de diciembre 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.