Prácticas comprobadas para desarrollar una estrategia multinube

AWS Guía prescriptiva

AWS Guía prescriptiva: Prácticas comprobadas para desarrollar una estrategia multinube

Table of Contents

Introducción 1
1. Alinee los objetivos multinube con su estrategia 3
Fusiones y adquisiciones 3
Deseo aprovechar las capacidades diferenciadas a largo plazo de otro CSP 4
Nube múltiple en la empresa matriz y nube principal en la empresa operadora o línea de negocio 4
2. Tenga en cuenta los conceptos erróneos sobre la multinube 6
Todo el mundo está adoptando estrategias multinube 6
La multinube reduce el riesgo de dependencia de un proveedor 6
La multinube mejora la disponibilidad y la resiliencia 8
La multinube ofrece mejores precios 9
3. Tenga una estrategia y una gobernanza claras que lo respalden 11
4. No distribuya las cargas de trabajo contiguas entre las nubes 14
5. Tenga una estrategia de integración a más largo plazo 15
6. Utilice los contenedores de forma estratégica 17
7. Tienes una sola CCo E, pero especialízate en ella 18
8. Asegúrese de que la seguridad sea siempre una prioridad 20
9. Adopte un enfoque de 80/20 sobre la distribución equitativa 22
Conclusión 24
Recursos 25
Historial de documentos 26
Glosario 27
..... 27
A 28
B 31
C 33
D 36
E 41
F 43
G 45
H 46
I 47
L 50
M 51

O 55
P 58
Q 61
R 61
S 64
T 68
U 70
V 71
W 71
Z 72
..... lxxiv

Prácticas comprobadas para desarrollar una estrategia multinube

Tom Godden y Ellie Tamari, Amazon Web Services

Septiembre de 2025 (historial del documento)

Hoy en día, las organizaciones se enfrentan a mensajes contradictorios sobre la adopción de la multinube. Algunos lo desaconsejan por completo, mientras que otros afirman que todo el mundo está cambiando a un entorno multinube. La realidad se encuentra entre estos extremos: existen razones legítimas a favor y en contra de las estrategias multinube, y el éxito depende de equilibrar el valor empresarial potencial con la complejidad y el riesgo inherentes.

En realidad AWS, nuestro compromiso con la interoperabilidad es una de las principales razones por las que muchos clientes eligen nuestra plataforma. Creemos en darle la libertad de innovar dondequiera que estén sus cargas de trabajo y en permitirle elegir la tecnología que mejor se adapte a sus necesidades. En AWS, hemos estado a la vanguardia del desarrollo de soluciones que le permiten crear e implementar aplicaciones en cualquier entorno. Este enfoque centrado en el cliente es fundamental para el Nube de AWS, en el que confían millones de clientes en todo el mundo.

Entendemos que los clientes necesitan plataformas en la nube que funcionen a la perfección tanto con las herramientas existentes como con las opciones tecnológicas del futuro. No debería tener que reconstruirlo todo cuando añada capacidades de otro proveedor. Su nube debería ayudarlo a conectar, proteger y administrar las cargas de trabajo en todos los entornos sin obligarlo a convertirse en un experto en todas las plataformas. AWS incorpora puntos de conexión directamente a sus servicios para ayudarle a operar de forma eficaz, ya sea que su estrategia consista en utilizarlos de AWS forma exclusiva o seguir un enfoque multicloud selectivo.

Reconocemos que cada organización tiene requisitos empresariales únicos que impulsan sus decisiones de estrategia de nube. Ya sea que ejecute cargas de trabajo principalmente en AWS varias nubes o las utilice AWS como parte de una arquitectura multinube más amplia, nos comprometemos a ayudarle a alcanzar el éxito. AWS ofrece todas las herramientas y capacidades necesarias para ayudarle a crear, migrar y operar con mayor facilidad y rapidez, independientemente de dónde residan sus cargas de trabajo. AWS las herramientas simplifican la administración entre los proveedores y, al mismo tiempo, maximizan el rendimiento y el valor de sus inversiones en la nube.

Este paper se centra en los principios comprobados para tener éxito con una estrategia multinube, incluyendo cuándo y dónde tiene sentido un enfoque multinube y cómo AWS ayuda a las empresas

a tener éxito con sus estrategias multinube. Proporciona una guía prescriptiva para ayudar a los ejecutivos a tomar decisiones informadas sobre la estrategia y la toma de decisiones relacionadas con la adopción de la multinube. Este paper no ofrece un análisis técnico en profundidad de las implementaciones multinube. Para obtener soporte técnico en materia de implementación y asistencia para sus desafíos específicos, le recomendamos que trabaje con su arquitecto de AWS soluciones.

Este paper presenta nueve principios comprobados para el éxito de la multinube basados en nuestras experiencias con clientes AWS empresariales. Cada principio aborda un aspecto fundamental de la estrategia multinube, desde la alineación de los objetivos empresariales hasta la implementación de la seguridad. Al aplicar estos principios, las organizaciones pueden afrontar la complejidad de la multinube con confianza.

- Principio 1. Alinee los objetivos de la multinube con su estrategia
- Principio 2. Tenga en cuenta los conceptos erróneos sobre la nube múltiple
- Principio 3. Tenga una estrategia y una gobernanza claras que lo respalden
- Principio 4. No distribuya las cargas de trabajo contiguas entre las nubes
- Principio 5. Tenga una estrategia de integración a más largo plazo
- Principio 6. Utilice los contenedores estratégicamente
- Principio 7. Tienen una sola CCo E, pero especialícense en ella
- Principio 8. Asegúrese de que la seguridad sea siempre una prioridad
- Principio 9. Adopte un enfoque de 80/20 sobre la distribución equitativa

Principio 1. Alinee los objetivos de la multinube con su estrategia

Los estudios de Gartner y las tendencias del sector muestran que las organizaciones adoptan cada vez más enfoques multinube para abordar necesidades empresariales específicas. Los siguientes escenarios demuestran cuándo una infraestructura multinube puede ser ventajosa desde el punto de vista estratégico.

Fusiones y adquisiciones

Las fusiones y adquisiciones (M&A) permiten tomar decisiones inmediatas sobre la estrategia de la nube. Si bien operar varias nubes puede aumentar los costos y la complejidad, una consolidación rápida puede retrasar el valor de la integración e interrumpir las operaciones comerciales. Sus decisiones sobre la nube se vuelven fundamentales para obtener los beneficios de las fusiones y adquisiciones.

La planificación de la integración debe tener en cuenta todo el panorama tecnológico. Cada carga de trabajo requiere una evaluación en el contexto del cronograma de integración y las prioridades empresariales.

Nuestra orientación:

- Desarrolle una estrategia de consolidación impulsada por la empresa que equilibre las necesidades de integración inmediatas con la eficiencia operativa a largo plazo. Inicialmente, mantenga múltiples nubes en circunstancias en las que una consolidación precipitada pueda interrumpir las operaciones comerciales críticas o retrasar la obtención del valor de las fusiones y adquisiciones.
- Cree criterios claros de asignación de las cargas de trabajo que se ajusten a su cronograma de integración. Priorice las aplicaciones generadoras de ingresos y los procesos empresariales principales, teniendo en cuenta las dependencias técnicas y los requisitos operativos.

Deseo aprovechar las capacidades diferenciadas a largo plazo de otro CSP

El miedo a quedarse fuera lleva a algunas empresas a querer disfrutar de todas las nubes. Las decisiones sobre la ubicación de las cargas de trabajo afectan a toda la organización, desde los equipos de ingeniería hasta las finanzas y las operaciones de seguridad.

Por lo tanto, las organizaciones deben examinar sus razones para buscar múltiples nubes. Algunos sostienen que cada carga de trabajo debe recaer en el proveedor de servicios en la nube (CSP) que mejor se adapte a sus necesidades. Sin embargo, la optimización de la carga de trabajo individual debe equilibrarse con el impacto organizacional más amplio. Cada proveedor de nube adicional corre el riesgo de aumentar la complejidad operativa, crear nuevos requisitos de talento e introducir consideraciones de seguridad que afecten a toda la organización tecnológica.

Nuestra orientación:

- Siga un enfoque 80/20: seleccione un proveedor principal para la mayoría de las cargas de trabajo y considere la posibilidad de contratar proveedores adicionales solo para casos de uso específicos y de gran valor. Esta estrategia maximiza la eficiencia y la retención del talento, a la vez que reduce la complejidad.
- Tenga en cuenta el costo total de operar en todas las nubes. Incluya en su análisis las herramientas de seguridad, los productos de gobierno, los sistemas de gestión financiera y los gastos operativos.
- Evalúe las dependencias e interacciones de cada carga de trabajo. Las cargas de trabajo rara vez funcionan de forma aislada; comparten datos, controles de seguridad y procesos operativos.
- Realice un análisis exhaustivo de la relación precio-rendimiento entre los proveedores. Compare no solo los costos directos, sino también los gastos generales de administrar varios entornos.

Nube múltiple en la empresa matriz y nube principal en la empresa operadora o línea de negocio

Las firmas de capital privado y las sociedades de cartera se enfrentan a consideraciones únicas sobre la estrategia de nube. Las empresas de su cartera suelen mantener estrategias de nube independientes, que suelen ser el resultado de actividades anteriores de fusiones y adquisiciones. Esta estructura reduce la complejidad que suele asociarse a las operaciones multinube, ya que cada unidad de negocio opera de forma independiente. Sin embargo, esta independencia puede limitar

las oportunidades de aprovechar los descuentos por volumen y los incentivos de compra en toda la empresa.

La eficacia de la estrategia de nube a nivel de sociedad holding depende de la autonomía de las empresas de cartera y de sus necesidades tecnológicas individuales. Si bien la consolidación puede generar un apalancamiento adquisitivo, puede entrar en conflicto con el modelo de operación independiente típico de las sociedades de cartera y las carteras de capital privado.

Nuestra orientación:

- Comprenda las estructuras de descuentos por volumen de los CSP. Cada proveedor ofrece mecanismos para añadir o eliminar filiales de los acuerdos empresariales y dividir las unidades de negocio en entidades independientes. Estos representan decisiones de doble sentido.
- Planifique cuidadosamente los compromisos de compra de la nube. Póngase en contacto con el equipo de cuentas de su CSP lo antes posible o póngase en contacto AWS Partner con un experto AWS en operaciones en la nube para obtener ayuda.
- Equilibre la independencia con la eficiencia. Considere la posibilidad de compartir servicios o acuerdos de compra que beneficien a las empresas en cartera sin limitar sus operaciones.
- Céntrese primero en los objetivos empresariales. Desarrolle estrategias tecnológicas que respalden su modelo operativo en lugar de seguir una estrategia multinube por sí sola.
- Evalúe las estrategias de nube desde el punto de vista de la gestión de carteras. Considere cómo las opciones de nube afectan a las posibles desinversiones o futuras adquisiciones.

Principio 2. Tenga en cuenta los conceptos erróneos sobre la nube múltiple

Cuando desarrolle su estrategia multinube, evite los conceptos erróneos habituales que se describen en las siguientes secciones.

Todo el mundo está adoptando estrategias multinube

Las firmas de asesoría y las empresas de medios presentan un panorama complejo en cuanto a la adopción de la multinube. Las investigaciones muestran un amplio interés por los enfoques multinube, pero los patrones de gasto suelen contar una historia diferente. En la práctica, muchas empresas mantienen entornos de nube única o relaciones claras con los primary/secondary CSP. Esta desconexión pone de relieve la importancia de ir más allá de los titulares y centrarse, en cambio, en las necesidades específicas de su organización.

Nuestra guía:

- Tome decisiones sobre la nube en función de sus requisitos empresariales específicos en lugar de seguir las tendencias del sector. Céntrese en los costos y riesgos cuantificables para su organización.
- Examine los casos de uso de la multinube en el contexto de su sector. Es posible que las estrategias de nube que funcionan para las empresas de tecnología de consumo no se traduzcan en entornos de servicios financieros, fabricación o juegos.
- Considere la gravedad de los datos como un factor principal a la hora de tomar decisiones sobre la ubicación de la carga de trabajo. La ubicación y el movimiento de los datos suelen determinar la arquitectura de nube más eficaz.
- Mire más allá de las estadísticas de adopción para comprender los patrones de gasto. Las altas tasas de adopción de la multinube notificadas a menudo ocultan los patrones de gasto reales.
- Evalúe las limitaciones técnicas antes de apostar por un entorno multinube. Algunas cargas de trabajo funcionan mejor cuando sus componentes permanecen en un único entorno de nube.

La multinube reduce el riesgo de dependencia de un proveedor

La flexibilidad de los proveedores es una consideración legítima en el desarrollo de la estrategia de nube. Las organizaciones valoran la capacidad de adaptar sus elecciones tecnológicas a medida que

evolucionan las necesidades empresariales. Esta preocupación refleja las experiencias anteriores con las inversiones en TI tradicionales, que generaron compromisos vinculantes a largo plazo. Los servicios en la nube ofrecen diferentes dinámicas en torno a la flexibilidad de los proveedores. AWS proporciona servicios compatibles con el código abierto y opciones de portabilidad de datos que reducen las barreras técnicas a la migración. Sin embargo, el equilibrio entre flexibilidad y eficiencia operativa sigue siendo importante. Las organizaciones deben sopesar el valor empresarial de mantener las opciones de los proveedores frente a las ventajas técnicas de una integración profunda con los servicios especializados de un proveedor principal.

Algunos clientes intentan evitar la dependencia diseñando soluciones independientes de la nube que utilizan contenedores. Este enfoque suele restringirlos a los servicios básicos de cómputo y almacenamiento, y evita las ventajas de las capacidades avanzadas de la nube. Nuestra experiencia demuestra que esta estrategia añade una complejidad considerable debido al aumento del tiempo de desarrollo y los recursos necesarios, en comparación con el uso de servicios nativos.

Nuestra orientación:

- Tenga en cuenta el coste total de las arquitecturas independientes de la nube. Es posible que la sobrecarga de ingeniería adicional no justifique las ventajas de la portabilidad.
- Utilice las capacidades nativas de la nube para obtener el máximo valor. Los servicios básicos de cómputo y almacenamiento por sí solos suelen sacrificar importantes ventajas en materia de seguridad, escalabilidad e innovación.
- Planifique estrategias de nube en función de los requisitos empresariales. Cuando una implementación multinube aporta un valor claro, como la capacidad de atender a los usuarios en múltiples plataformas, la inversión adicional en ingeniería vale la pena.
- Evalúe los escenarios de salida y los costes realistas. Compare la probabilidad y los gastos de cambiar de proveedor con los beneficios de utilizar el conjunto completo de Servicios de AWS.
- Aproveche los fundamentos del código abierto de AWS. AWS los servicios gestionados, como Amazon Relational Database Service (Amazon RDS), le proporcionan flexibilidad y excelencia operativa y son compatibles con los motores de bases de datos que utiliza actualmente.
- Aproveche las completas herramientas de migración que ofrece. AWS Le ayudamos a mover las cargas de trabajo en cualquier dirección y le ofrecemos una salida de datos gratuita si opta AWS por otros proveedores. Para obtener más información, consulte la entrada del AWS blog Transferencia gratuita de datos a Internet al salir de ella. AWS

La multinube mejora la disponibilidad y la resiliencia

La creencia en la posibilidad de cambiar la carga de trabajo de un proveedor de nube a otro durante las interrupciones impulsa a algunas organizaciones a adoptar estrategias multinube. Esta mentalidad crea una visión demasiado simplificada de la resiliencia de la infraestructura de nube que ignora las realidades técnicas fundamentales.

Tras años de experiencia trabajando con clientes multinube AWS, hemos comprobado que mantener la portabilidad total de las cargas de trabajo entre proveedores suele generar una complejidad considerable sin ofrecer todos los beneficios esperados. Las aplicaciones con un uso intensivo de datos se enfrentan a desafíos insuperables debido a las limitaciones de la gravedad de los datos. De hecho, en nuestra opinión, es casi imposible que las organizaciones implementen con éxito una conmutación por error multinube realmente perfecta para cargas de trabajo con un uso intensivo de datos.

Lydia Leong, distinguida vicepresidenta analista de Gartner, refuerza esta perspectiva en una publicación en las redes sociales: «La conmutación por error multinube es compleja y costosa, hasta el punto de que casi siempre resulta poco práctica y no es una forma especialmente eficaz de abordar los riesgos de resiliencia de la nube». La diferencia inherente entre los proveedores en materia de redes, almacenamiento, bases de datos, aprendizaje automático y seguridad hace que la verdadera portabilidad sea prácticamente imposible. Distribuir las cargas de trabajo entre los proveedores puede aumentar el riesgo, ya que una falla en cualquiera de los entornos podría provocar una interrupción en todos los entornos.

Nuestra guía:

- Concéntrese en dominar AWS las capacidades de las cargas de trabajo individuales en lugar de optar por arquitecturas multinube complejas.
- Aumente la resiliencia a través de Regiones de AWS las zonas de disponibilidad en lugar de intentar la conmutación por error entre proveedores. Para obtener información técnica detallada sobre cómo AWS realizar la conmutación automática por error de las cargas de trabajo entre centros de datos físicos, consulte la entrada del AWS blog titulada Zonal autoshift: aleja automáticamente el tráfico de las zonas de disponibilidad cuando detectamos posibles problemas.
- Migre las cargas de trabajo de forma estratégica y concéntrese en una aplicación a la vez para maximizar el éxito. AWS

La multinube ofrece mejores precios

La competitividad de los precios puede ser el argumento más débil de todos a favor de los entornos multinube. Las experiencias de las organizaciones con contratos de software o centros de datos complicados y costosos que las obligan a celebrar acuerdos de varios años las han hecho desconfiar a la hora de adquirir servicios de TI. Los enfoques de adquisición tradicionales no se han adaptado a las pay-as-you-go compras, a los descuentos por volumen ni a la realidad de la competencia de precios en la nube. (En enero de 2025, AWS ha reducido los precios 151 veces desde su creación).

El principal factor de reducción de costes es un entorno de nube bien gestionado y optimizado. Una empresa optimiza mejor los costes si trabaja principalmente con un proveedor cuyos servicios ofrecen ventajas en cuanto a precio y rendimiento (como las instancias de cómputo que se basan en chips diseñados a medida, como AWS Graviton) y que cuenta con soluciones superiores de gestión financiera en la nube. Según un estudio de Hackett Group realizado en 2022 con más de 1000 organizaciones, el gasto en infraestructura como porcentaje del gasto total en TI fue un 20% inferior en el caso de los clientes en comparación con las organizaciones multinube. AWS

Nuestra experiencia ha demostrado que las empresas no prevén el coste y la complejidad adicionales que supone operar en varias nubes, ni comparan adecuadamente este coste con el beneficio percibido si se head-to-head contratan proveedores.

Nuestra orientación:

- Desarrolle su estrategia de optimización de costos sobre el pilar de optimización de costos de AWS Well-Architected Framework. Existen cinco principios de diseño:
  - Implemente la gestión financiera en la nube: para lograr el éxito financiero y acelerar la obtención de valor empresarial en la nube, debe invertir en la gestión financiera en la nube. Su organización debe dedicar el tiempo y los recursos necesarios para desarrollar capacidades en este nuevo ámbito de la tecnología y de administración del uso. Al igual que con su capacidad de seguridad u operaciones, necesita ampliarlas mediante la creación de conocimientos, programas, recursos y procesos para convertirse en una organización rentable.
  - Adopte un modelo de consumo: pague solo por los recursos de computación que utilice y aumente o reduzca el uso según los requisitos del negocio. Por ejemplo, los entornos de desarrollo y prueba se utilizan normalmente solo ocho horas al día durante la semana laboral. Puede detener estos recursos cuando no estén en uso para obtener un ahorro potencial de costes del 75% (40 horas frente a 168 horas).

  - Mida la eficiencia general: mida el rendimiento empresarial de su carga de trabajo y los costes asociados a la entrega. Use estos datos para comprender las ganancias que obtiene al aumentar la producción, aumentar la funcionalidad y reducir los costos.
  - Deje de gastar dinero en tareas pesadas e indiferenciadas: CSPs haga el trabajo pesado de las operaciones del centro de datos, como almacenar, apilar y alimentar los servidores. También eliminan la carga operativa que supone administrar los sistemas operativos y las aplicaciones mediante el uso de servicios gestionados. Esto le permite centrarse en sus clientes y proyectos empresariales en lugar de centrarse en la infraestructura de TI.
  - Analice y atribuya los gastos: la nube facilita la identificación precisa del uso y el costo de las carga de trabajo, lo que permite atribuir de forma transparente los costos de TI a fuentes de ingresos y propietarios de cargas de trabajo individuales. Esto lo ayuda a medir el retorno de la inversión (ROI) y da a los propietarios de cargas de trabajo la oportunidad de optimizar sus recursos y reducir costos.
- Dada la sobrecarga financiera que supone operar con distintos proveedores, orientamos a los clientes para que inviertan fuertemente en herramientas de automatización y optimización de costes. Cada CSP ofrece amplias herramientas nativas en esta área, como la. Centro de optimización de costes de AWS La mayoría de las herramientas nativas ofrecen excelentes capacidades a los clientes en su entorno de nube. Sin embargo, para entender el gasto en múltiples CSPs, puede elegir entre un amplio conjunto de ISV y productos de software como servicio (SaaS) que amplían estas capacidades para proporcionar una experiencia única para la optimización de costos.
- Diluir el poder adquisitivo mediante una estrategia de inversión en capital no genera valor empresarial. Puede socavar los posibles descuentos por volumen y, potencialmente, socavar el diseño técnico. La forma más eficiente de consumir los servicios en la nube es utilizar un proveedor principal para la mayor parte de sus operaciones y utilizar otros CSPs solo cuando esto añada valor empresarial.

Principio 3. Tenga una estrategia y una gobernanza claras que lo respalden

Decidir seguir una estrategia multinube no es suficiente; debe establecer una estrategia para cumplir sus objetivos, incluida una gobernanza clara sobre qué cargas de trabajo se destinarán a dónde y por qué. Los criterios de evaluación se deben utilizar para optimizar las cargas de trabajo y sus dependencias. Si la evaluación se deja en manos de las personas, es probable que una dispersión descoordinada entre todos los participantes CSPs disminuya el valor de la estrategia multinube. Le recomendamos que evalúe el rendimiento de la carga de trabajo del CSP con regularidad y que utilice su evaluación como información clave para la selección, los criterios y el uso futuro del CSP.

Una estrategia de gobierno eficaz requiere la visibilidad del número total de servicios, aplicaciones y componentes que se utilizan en la empresa. Para ello, es fundamental contar con una estrategia de etiquetado sólida que abarque CSPs y establezca claramente la propiedad, el uso y el entorno (como el desarrollo, el control de calidad, la preparación y la producción) para todos los recursos desplegados. Todo debe estar etiquetado a nombre de un propietario; si no está etiquetado o no se puede identificar a un propietario, se debe quitar. Trabajamos en estrecha colaboración con una importante organización de servicios financieros que encuentra y elimina automáticamente cualquier recurso sin etiquetar, y lo considera una buena práctica, independientemente de las molestias que ello suponga para los equipos de desarrollo. Este enfoque de etiquetado codifica las normas de gobernanza y automatiza su aplicación en lugar de obstaculizar el progreso (es decir, implementa barreras, no barreras). Los costes, las operaciones y la seguridad deben rastrearse, supervisarse y gestionarse de la misma manera, con la misma profundidad de datos y con la misma transparencia. CSPs

Al implementar una estrategia multinube, establecer una estructura contable clara y coherente entre los proveedores de servicios en la nube es crucial para mantener el control y la seguridad operativos. Recomendamos adoptar un hub-and-spoke modelo en el que se creen unidades de negocio independientes Cuentas de AWS para las diferentes. Están anclados en dos cuentas centrales fundamentales: una security/audit cuenta para la supervisión consolidada del cumplimiento y la seguridad, y una cuenta de red central para gestionar la interconectividad. (Este enfoque está codificado en el diseño de. AWS Control Tower Sin embargo, los principios de privilegio mínimo y separación de funciones se aplican igualmente a otras nubes. El AWS Well-Architected Framework analiza estos conceptos en detalle y es muy recomendable para el público técnico.) Este enfoque fundamental debe reflejarse en todos los proveedores de servicios en la nube para mantener la coherencia en la gobernanza y las operaciones. Las cuentas de carga de trabajo deben organizarse

por entorno (desarrollo, puesta en escena, producción) o función, con procesos claros establecidos para la creación y eliminación de cuentas.

Nuestra guía:

- Implemente una estrategia de etiquetado integral para mantener patrones de propiedad y uso claros en todos los recursos de la nube. Realice un seguimiento de los entornos, los centros de costes, las aplicaciones y las unidades de negocio mediante políticas de etiquetado coherentes. Elimine los recursos que carezcan de las etiquetas adecuadas para hacer cumplir los estándares de gobierno y mantener la claridad del entorno.
- Establezca un marco de cumplimiento unificado que mapee los requisitos normativos en su entorno multinube. Lleve una documentación clara sobre cómo los controles y las certificaciones de cada proveedor de nube respaldan sus obligaciones de cumplimiento.
- Automatice la aplicación de la gobernanza mediante la automatización en lugar de utilizar procesos de aprobación manuales. Codifique sus reglas de gobierno en sistemas automatizados que eviten las infracciones de las políticas antes de que se produzcan. Esto elimina los errores humanos y, al mismo tiempo, mantiene la velocidad de desarrollo.
- Estructure las cuentas en un hub-and-spoke modelo con control centralizado de seguridad y redes. Cree cuentas dedicadas a la auditoría de seguridad y la administración de la red a fin de centralizar las funciones críticas. Esta base permite políticas de seguridad y conectividad de red coherentes en toda la organización.
- Para mantener los límites operativos, cree cuentas, suscripciones o proyectos separados (según la nomenclatura de su CSP) para diferentes entornos y funciones. Divida las cargas de trabajo por entornos de desarrollo, puesta en escena y producción. Esta separación evita que los incidentes de seguridad se propaguen y mantiene claros los dominios operativos.
- Supervise los costes, las operaciones y la seguridad mediante métricas coherentes en todo el entorno. Implemente un monitoreo unificado para la utilización de los recursos, los eventos de seguridad y los patrones de gasto. Utilice estos datos para optimizar las decisiones sobre la ubicación de la carga de trabajo y la asignación de recursos.
- Evite el uso no autorizado de la nube mediante políticas organizativas y controles automatizados. Defina procesos claros para la creación de cuentas y el aprovisionamiento de recursos. Implemente políticas de control de servicios (SCPs) para garantizar el cumplimiento de los estándares organizacionales en todas las cuentas.
- Establezca controles preventivos y de detección para evitar que la TI clandestina aparezca a través de cuentas de proveedores no autorizados. Supervise el uso no autorizado de la nube

mediante informes de gastos y tráfico de red. Bloquee el acceso de proveedores no autorizados y, al mismo tiempo, mantenga las vías de innovación aprobadas.

Principio 4. No distribuya las cargas de trabajo contiguas entre las nubes

Distribuir las cargas de trabajo contiguas entre varios proveedores de nube genera complejidad, riesgo y costo innecesarios. Cuando las cargas de trabajo que procesan y analizan datos en conjunto abarcan varios proveedores, las organizaciones se enfrentan a desafíos relacionados con el movimiento, la sincronización y la coherencia de los datos. Los equipos deben utilizar diferentes interfaces de administración APIs, modelos de seguridad y procesos operativos para cada proveedor, lo que aumenta la probabilidad de errores y aumenta la sobrecarga operativa. Esta complejidad aumenta las probabilidades de errores y la sobrecarga operativa, y puede dificultar la agilidad y la escalabilidad.

Sin embargo, en algunos escenarios prácticos, es posible que las organizaciones necesiten distribuir las cargas de trabajo contiguas entre las nubes debido a requisitos empresariales o técnicos específicos. En estos casos, le recomendamos que establezca criterios y principios rectores claros para evaluar las ventajas y desventajas y garantizar que el enfoque se alinee con la estrategia multinube general de su organización.

Cuando las organizaciones optan por distribuir las cargas de trabajo en varias nubes, adoptar una arquitectura que se centre en la mensajería y en un acoplamiento flexible puede aliviar muchos de los desafíos asociados. Esta es la mejor manera de separar las preocupaciones de las nubes y reducir el alcance del impacto en caso de que un proveedor tenga alguna discapacidad. Lo ideal sería que las operaciones con plazos más limitados, como las transacciones financieras, se mantuvieran en un entorno único. Nunca se debe permitir que una interrupción en un entorno ponga en peligro las cargas de trabajo en otro entorno.

Nuestra guía:

- Diseñe cargas de trabajo en la nube para lograr la independencia operativa y minimizar las dependencias en tiempo real entre los proveedores. Cuando sea necesaria la distribución de la carga de trabajo, implemente mecanismos eficientes de transferencia masiva de datos en lugar de mantener conexiones constantes entre nubes.
- Evalúe cada carga de trabajo distribuida propuesta en función de criterios empresariales claros. Tenga en cuenta tanto los beneficios estratégicos como la complejidad operativa que introduce la distribución.

Principio 5. Tenga una estrategia de integración a más largo plazo

Tenga cuidado al mover grandes volúmenes de datos entre aplicaciones de diferentes nubes, especialmente si sus aplicaciones y recursos informáticos se implementan en un CSP y los recursos de almacenamiento de datos se implementan en otro. Esta situación puede añadir complejidad y latencia que podrían compensar los beneficios percibidos. Hablamos con muchos clientes que tienen un lago de datos en una nube, pero desean realizar análisis o aprendizaje automático (ML) con herramientas de otro CSP. Decidir dónde colocar las cargas de trabajo en un entorno multinube es una de las decisiones más importantes y, a menudo, más desafiantes a las que se enfrentan las organizaciones. Le recomendamos que evalúe cada decisión de ubicación de la carga de trabajo en función de tres dimensiones fundamentales: los requisitos técnicos, las necesidades empresariales y los puntos fuertes de los proveedores.

Comience las evaluaciones técnicas mapeando las características esenciales de cada carga de trabajo: potencia de cómputo, operaciones de datos, necesidades de tiempo de respuesta y requisitos de crecimiento. Naturalmente, las aplicaciones funcionan mejor cuando se encuentran cerca de sus datos. Alejar las aplicaciones de sus fuentes de datos crea obstáculos técnicos innecesarios y reduce el rendimiento.

Las decisiones empresariales deben tener en cuenta los precios de los proveedores, los requisitos de residencia de los datos y los contratos con los proveedores. Cada ubicación de la carga de trabajo afecta a las operaciones, la seguridad y la productividad de toda la organización. Al analizar las cargas de trabajo de forma aislada, se toman decisiones subóptimas.

Nuestra orientación:

- Implemente la transferencia masiva de datos entre nubes en lugar del acceso en tiempo real. Programe la actualización periódica de los datos mediante operaciones masivas eficientes en lugar de utilizar llamadas constantes a la API entre nubes. Este enfoque reduce los costos, mejora la confiabilidad y mantiene un rendimiento constante. Por ejemplo, exporte datos resumidos de ventas diarias en lugar de consultar transacciones individuales en las nubes.
- Tenga en cuenta la gravedad de los datos al diseñar la ubicación de las cargas de trabajo Mantenga las aplicaciones cerca de sus fuentes de datos principales para mantener el rendimiento y reducir los costos. Los modelos de aprendizaje automático, los motores de análisis y los sistemas de procesamiento de transacciones se benefician del acceso directo a sus datos. Alejar estas cargas de trabajo de sus datos crea una latencia y una complejidad innecesarias en la red.

- Evalúe las decisiones sobre las cargas de trabajo en el contexto de su estrategia de nube completa, en lugar de revisarlas de forma aislada. Considere cómo afecta cada elección de ubicación a los procesos operativos, los controles de seguridad y las capacidades de los equipos en toda su organización. Una decisión que parezca óptima para una sola carga de trabajo puede complicar la supervisión o aumentar los riesgos de seguridad si se analiza de forma integral.
- Defina políticas claras de propiedad y gobierno de los datos que especifiquen dónde pueden residir los diferentes tipos de datos. Cree un marco de clasificación de datos que impulse decisiones coherentes sobre la ubicación de los datos entre los proveedores de servicios en la nube.

Principio 6. Utilice los contenedores estratégicamente

Los contenedores pueden desempeñar un papel valioso a la hora de respaldar una estrategia multinube, pero también es importante reconocer sus limitaciones. El uso de contenedores suele ser una buena idea para cualquier aplicación moderna nativa de la nube, ya que ofrecen ventajas en cuanto a portabilidad y coherencia en distintos entornos. Los contenedores son independientes de la plataforma, lo que significa que pueden ejecutarse en cualquier plataforma o infraestructura de nube que admita la tecnología de contenedorización, como Kubernetes. Organismos que utilizan contenedores pueden desarrollar y empaquetar sus aplicaciones una vez y, después, desplegarlas de forma coherente en varios proveedores de nube o entornos locales, sin necesidad de realizar modificaciones importantes. Al encapsular el código de la aplicación, las dependencias y el entorno de ejecución en un contenedor, puede lograr un alto grado de portabilidad, lo que le permite mover las cargas de trabajo sin problemas entre los proveedores de la nube o entre la nube y los centros de datos locales.

Sin embargo, es posible que los contenedores no resuelvan todos los casos de uso ni eliminen todos los desafíos a los que podría enfrentarse una organización a la hora de adoptar una estrategia multinube. Los contenedores funcionan mejor con arquitecturas modernas basadas en microservicios, pero es posible que no sean tan adecuados para aplicaciones monolíticas de gran tamaño. Además, aunque los contenedores pueden abordar ciertos aspectos de la portabilidad, como el tiempo de ejecución de las aplicaciones, no resuelven automáticamente los problemas relacionados con la administración de datos, las políticas de seguridad y otras dependencias entre nubes. Las organizaciones aún deben planificar y diseñar cuidadosamente sus soluciones multinube para garantizar una administración de datos coherente, controles de seguridad unificados y una integración perfecta entre los componentes alojados en la nube y los locales.

Nuestra orientación:

- Utilice las capacidades de administración de contenedores nativas de cada proveedor de servicios en la nube para maximizar el valor empresarial y acelerar la entrega. Este enfoque garantiza un rendimiento óptimo y, al mismo tiempo, evita la complejidad de crear soluciones independientes de la nube que rara vez ofrecen retornos significativos.
- Desarrolle estrategias de contenedores que aborden el panorama operativo completo, incluida la administración de datos, la seguridad y las dependencias entre nubes. Céntrese en los resultados empresariales cuando tome decisiones sobre la arquitectura de contenedores.

Principio 7. Ten una sola CCo E, pero especialízate en ella

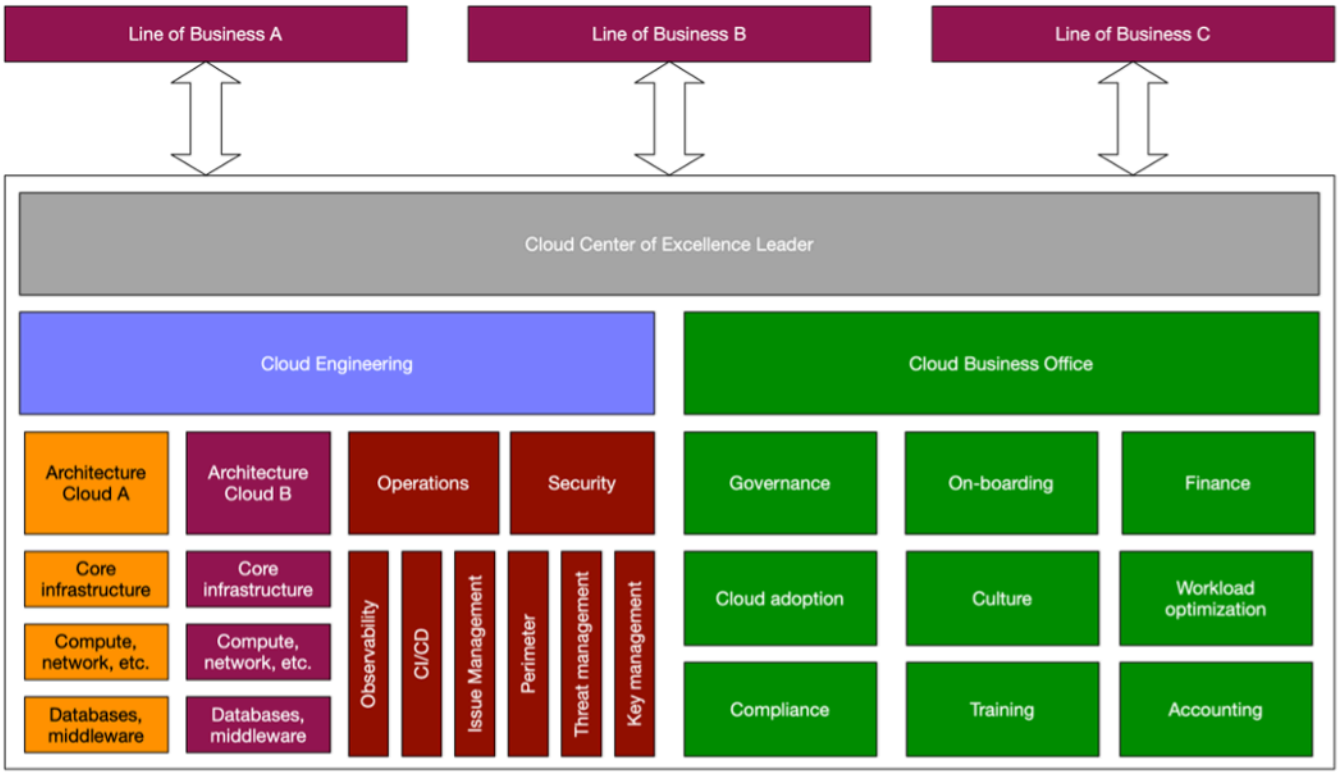
Como aconsejamos AWS a muchos clientes, debería crear un centro de excelencia (CCoE) en la nube dentro de su organización para proporcionar liderazgo, estandarización y aceleración de su transición a la nube. En lo que respecta a los entornos multinube, observamos que las empresas más exitosas adoptan un enfoque equilibrado con sus soluciones E. CCo

En lugar de establecer una CCo E separada para cada CSP, le recomendamos que tenga una CCo E única y unificada que supervise la estrategia multinube de la organización. Esto ayuda a garantizar un enfoque coordinado y coherente, en lugar de esfuerzos aislados que pueden provocar divergencias, reingeniería y despilfarro. Asegúrese de que los equipos de su única CCo E cuenten con las habilidades, herramientas y mecanismos especializados necesarios para cada CSP que utilice su organización. Estos conocimientos especializados permiten a la CCo E gestionar, respaldar y acelerar el uso de las diferentes plataformas en la nube de forma eficaz.

Por ejemplo, la CCo E debe contar con expertos AWS específicos que comprendan en profundidad los Nube de AWS servicios y las mejores prácticas, así como expertos en el caso de otros expertos CSPs que puedan guiar el uso de esas tecnologías de nube por parte de la organización. Esta experiencia especializada dentro de una única CCo E puede ayudar a su organización a beneficiarse de la coordinación y la estandarización de un enfoque centralizado y, al mismo tiempo, garantizar que cada plataforma en la nube se utilice de manera óptima.

La CCo E única debería ser el órgano rector central que establezca los estándares, las políticas y las mejores prácticas para la estrategia multinube de la organización. La implementación real de las cargas de trabajo y los proyectos en la nube se puede distribuir a equipos o unidades de negocio especializados, mientras que el CCOE se encarga de la supervisión, el apoyo y la coordinación. Este enfoque equilibrado ayuda a garantizar una estrategia multinube cohesiva y, al mismo tiempo, proporciona el grado necesario de flexibilidad y autonomía dentro de la organización.

El siguiente diagrama ilustra cómo una CCo E puede proporcionar un enfoque y una gobernanza centralizados en múltiples líneas de negocio (LOBs), equipos de ingeniería en la nube y equipos de oficinas comerciales en la nube (CBO).



Nuestra guía:

- Estructure su CCo E para mantener una supervisión estratégica y, al mismo tiempo, incorpore la experiencia especializada de cada proveedor de servicios en la nube. Céntrese en contratar a expertos expertos en plataformas cloud individuales, en lugar de buscar especialistas en multinube poco comunes, y fomente el intercambio interno de conocimientos para desarrollar las capacidades organizativas.
- Capacite a su CCo empresa electrónica para establecer estándares en toda la empresa en relación con cuestiones transversales como la seguridad y la observabilidad, al tiempo que proporciona a los equipos individuales la autonomía necesaria para ejecutar estas directrices mediante el uso de herramientas y servicios nativos de la nube.
- Desarrolle una estrategia integral de talento que equilibre una amplia experiencia en las plataformas de nube principales con un conocimiento arquitectónico más amplio. Céntrese en crear equipos que combinen sólidas habilidades específicas de la nube con experiencia en arquitectura empresarial.

Principio 8. Asegúrese de que la seguridad sea siempre una prioridad

Un enfoque multinube hace que sea más difícil garantizar la seguridad al aumentar el riesgo de acceso no autorizado, ya que su postura de seguridad debe tener en cuenta más superficies de ataque. Una estrategia multinube suele obligar a las empresas a utilizar varios modelos de seguridad CSPs en áreas como la gestión de identidades, la seguridad de las redes, la gestión de activos y el registro de auditorías. Esta complejidad corre el riesgo de dificultar la transparencia, aumentar la carga para los equipos de seguridad y aumentar el riesgo.

La automatización de la seguridad es esencial en los entornos multinube. La gestión de identidades debe funcionar sin problemas en todos los entornos; debe conectar a los proveedores de identidad existentes y, al mismo tiempo, mantener políticas de acceso coherentes. La seguridad requiere una protección integrada en todos los niveles de datos, redes y terminales. La clasificación de los datos, el cifrado y la gestión del ciclo de vida constituyen la base. La seguridad de la red se basa en diseños y patrones de conexión estandarizados. La protección de terminales completa el marco mediante una gestión de parches coherente y controles basados en el host.

Estos elementos fundamentales son fundamentales para la adopción exitosa y segura de varios proveedores de nube y deben tenerse en cuenta al principio de cualquier planificación de una estrategia multinube.

Nuestra orientación:

- Implemente un marco de seguridad integrado en su entorno multinube que se centre en tres elementos principales: la protección de los datos mediante la clasificación y el cifrado estandarizados, la seguridad de la red mediante patrones de diseño coherentes y la protección de los terminales mediante controles sistemáticos y la administración de parches.
- Establezca un modelo de operaciones de seguridad unificado que aproveche las capacidades de seguridad nativas de cada proveedor de nube y, al mismo tiempo, mantenga la visibilidad y el control centralizados mediante herramientas y procesos estandarizados.
- Centralice la recopilación y el análisis de datos de seguridad mediante Amazon Security Lake. Esta plataforma agrega información de seguridad de AWS otros proveedores de nube, aplicaciones SaaS y sistemas locales en una sola vista. Es compatible con el Open Cybersecurity Schema Framework (OCSF) y permite un análisis estandarizado en su entorno híbrido y multinube. Este

enfoque centralizado mejora la detección y la respuesta a las amenazas y, al mismo tiempo, simplifica las operaciones de seguridad.

- Implemente las herramientas de seguridad nativas de cada proveedor para mejorar sus capacidades de protección. Estos servicios diseñados específicamente abordan las funciones específicas del proveedor y, al mismo tiempo, devuelven los datos a su plataforma de seguridad centralizada. Una combinación de herramientas nativas y visibilidad centralizada ayuda a proporcionar una cobertura de seguridad integral en toda la infraestructura.
- Implemente una estrategia de observabilidad unificada que proporcione una visibilidad completa de todo su entorno de nube, incluidos los datos operativos y de seguridad, desde cero. Estandarice los enfoques de monitoreo líderes del sector que permiten un seguimiento uniforme de los servicios empresariales, independientemente de dónde operen.
- Establezca estándares empresariales para la recopilación y visualización de datos operativos que permitan identificar y resolver problemas rápidamente en su entorno multinube. Céntrese en crear una fuente única de información fiable sobre las operaciones que sirva tanto a las partes interesadas técnicas como empresariales.

Principio 9. Adopte un enfoque 80/20 sobre la distribución equitativa

La forma en que distribuya las cargas de trabajo entre los proveedores determina fundamentalmente su éxito multinube. Muchas organizaciones persiguen por error la igualdad en su distribución de la nube e intentan distribuir las cargas de trabajo de manera uniforme entre los proveedores. Este enfoque aumenta la complejidad sin ofrecer beneficios proporcionales. La distribución equitativa fragmenta sus capacidades técnicas, diluye su poder adquisitivo y genera una sobrecarga operativa innecesaria. Los equipos se esfuerzan por desarrollar una amplia experiencia cuando se ven obligados a mantener la competencia en múltiples plataformas simultáneamente.

El enfoque 80/20 ofrece resultados claramente mejores que una distribución equitativa entre las nubes. Al concentrar el 80% de su inversión en un proveedor principal y utilizar otros de forma selectiva para funciones específicas, se crea una estrategia equilibrada que reduce tanto los costes como la complejidad. Este enfoque concentrado acelera la innovación porque sus equipos pueden desarrollar una amplia experiencia con los servicios avanzados de su plataforma principal. Su personal técnico puede convertirse en especialista en una arquitectura en lugar de mantener un conocimiento superficial en varios entornos. Cuando los ingenieros dominan una plataforma, crean de manera más eficiente, solucionan problemas más rápido e implementan soluciones más sofisticadas.

Las empresas que siguen el enfoque 80/20 suelen retener mejor el talento porque sus equipos adquieren una experiencia valiosa y comercializable, en lugar de tener que trabajar con múltiples tecnologías. Esta estrategia concentrada también ayuda a simplificar la gestión de la seguridad al limitar la complejidad de los diferentes modelos de seguridad de los distintos proveedores. La nube principal recibe la mayor parte de su inversión en herramientas de seguridad, soluciones de monitoreo y procesos operativos. Esto crea una base de seguridad más sólida de lo que es posible con recursos divididos en partes iguales.

Nuestra guía:

- Seleccione un proveedor de nube principal que se ajuste a la mayoría de sus requisitos comerciales y técnicos. Este proveedor debería soportar al menos el 80% de sus cargas de trabajo y convertirse en la base de su estrategia de nube. Centra tus inversiones en formación, estándares de arquitectura y procesos operativos en maximizar el valor de esta plataforma principal.
- Desarrolle criterios claros para las cargas de trabajo que justifiquen su ubicación en nubes secundarias. Estos criterios deben centrarse en el valor empresarial específico que su proveedor

principal no puede lograr. Evite colocar las cargas de trabajo en nubes secundarias simplemente para mantener la equidad en el gasto o el equilibrio artificial entre los proveedores.

- Estructure sus acuerdos empresariales para que reflejen su enfoque 80/20. Negocie descuentos por volumen con su proveedor principal en función de la concentración de gastos y mantenga la flexibilidad con los proveedores secundarios para casos de uso específicos. Este enfoque maximiza su apalancamiento de compras y, por lo general, se traduce en mejores precios generales que dividir el gasto en partes iguales.
- Alinee su estrategia de talento con su enfoque 80/20. Invierta en desarrollar una amplia experiencia con los servicios de su proveedor principal y, al mismo tiempo, mantenga un conocimiento suficiente de las plataformas secundarias para soportar cargas de trabajo específicas. Esta estrategia centrada en el talento mejora la productividad, acelera la prestación de servicios y reduce el riesgo de que se produzcan carencias de competencias críticas.
- Mida periódicamente los resultados empresariales de su estrategia multinube. Realice un seguimiento de las métricas que demuestran el valor obtenido de cada proveedor y ajuste su distribución si es necesario. El objetivo no es evitar por completo la multinube, sino implementarla estratégicamente donde cargas de trabajo específicas se beneficien realmente de las capacidades que son exclusivas de otros proveedores.

Conclusión

En este paper se describen nueve principios clave para desarrollar una estrategia multicloud eficaz. Las organizaciones logran el mayor éxito a través de un enfoque de nube primaria con el uso estratégico de proveedores adicionales cuando las necesidades empresariales específicas lo exigen. El enfoque 80/20 que hemos descrito equilibra la concentración con la flexibilidad y permite a las organizaciones desarrollar una experiencia más profunda, mantener relaciones más sólidas con los proveedores y crear talentos más valiosos, sin dejar de satisfacer los requisitos legítimos de la multinube.

La implementación exitosa de la multinube requiere una evaluación clara de las necesidades empresariales en lugar de seguir las tendencias del sector. Las empresas deben establecer una gobernanza sólida, mantener la seguridad como una de las principales prioridades, evitar repartir las cargas de trabajo conectadas entre los proveedores, conservar las aplicaciones con sus datos transaccionales, reconocer las limitaciones de los contenedores y mantener un centro de excelencia en la nube unificado pero especializado.

El AWS enfoque de la nube se basa fundamentalmente en la capacidad de elección del cliente y en la interoperabilidad. Hemos diseñado nuestras herramientas y servicios para que funcionen sin problemas en todos los entornos porque entendemos que las necesidades de su empresa suelen ir más allá de un único proveedor. Desde soluciones de conectividad híbridas hasta la organización de contenedores que abarca distintos entornos, AWS ofrece funcionalidades que le ayudan a operar de forma eficaz en todo su entorno tecnológico.

En lugar de obligarlo a convertirse en un experto en múltiples plataformas, AWS simplifica la administración multinube mediante herramientas intuitivas e interfaces coherentes. Nos centramos en eliminar la complejidad para que usted pueda centrarse en la innovación. Estas capacidades lo ayudan a implementar su estrategia multinube según sus propios términos, ya sea que se trate de un entorno AWS exclusivo o específico Servicios de AWS junto con otros entornos.

La nube debería potenciar su estrategia empresarial, no limitarla. Al aplicar los principios descritos en este paper y aprovechar las capacidades de AWS interoperabilidad, puede crear un enfoque de nube que maximice el valor, minimice la complejidad innecesaria y posicione a su organización para el éxito a largo plazo en el dinámico entorno empresarial actual.

Para obtener más información sobre AWS las soluciones que pueden ayudar a simplificar la administración en entornos híbridos y multinube, consulte las soluciones para multinube.AWS

Recursos

Referencias

- Uso de un centro de excelencia (CCOE) en la nube para transformar toda la empresa (AWS entrada del blog)
- AWS Marco de buena arquitectura
- Identificación de oportunidades con Cost Optimization Hub (AWS Cost Management documentación)
- El valor empresarial de la migración a Amazon Web Services (The Hackett Group, febrero de 2022)
- Transferencia gratuita de datos a Internet al salir de ella AWS(AWS entrada del blog)

Herramientas

- Cambio automático zonal: aleja automáticamente el tráfico de las zonas de disponibilidad cuando detectemos posibles problemas (AWS entrada del blog)
- AWS soluciones para multinube

AWS Socios

- Nube de AWS Competencia operativa

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	—	3 de septiembre de 2025

AWS Glosario de orientación prescriptiva

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

Números

Las 7 R

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

- Refactorizar/rediseñar: traslade una aplicación y modifique su arquitectura mediante el máximo aprovechamiento de las características nativas en la nube para mejorar la agilidad, el rendimiento y la escalabilidad. Por lo general, esto implica trasladar el sistema operativo y la base de datos. Ejemplo: Migrar la base de datos de Oracle en las instalaciones a Amazon Aurora PostgreSQL-Compatible Edition.
- Redefinir la plataforma (transportar y redefinir): traslade una aplicación a la nube e introduzca algún nivel de optimización para aprovechar las capacidades de la nube. Ejemplo: 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: Migrar el sistema de administración de las relaciones con los clientes (CRM) a Salesforce.com.
- Volver a alojar (migrar mediante lift-and-shift): traslade una aplicación a la nube sin realizar cambios para aprovechar las capacidades de la nube. Ejemplo: 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

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.

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 AIOps se utiliza en la estrategia de AWS migración, consulte la guía de integración de operaciones.

cifrado asimétrico

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

atomicidad, consistencia, aislamiento, durabilidad (ACID)

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

control de acceso basado en atributos (ABAC)

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

origen de datos fidedigno

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

Zona de disponibilidad

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

AWS Marco de adopción de la nube (AWS CAF)

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

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

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

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

B

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.

implementación azul/verde

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 más información, consulte el indicador Implement break-glass procedures en la guía de AWS Well-Architected.

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.

cifrado del cliente

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

Centro de excelencia en la nube (CCoE)

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

computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar 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: realizar inversiones fundamentales para escalar su adopción de la nube (p. ej., crear una landing zone, definir una CCo E, establecer un modelo de operaciones)

- Migración: migración de aplicaciones individuales
- Reinvención: optimización de productos y servicios e innovación en la nube

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

CMDB

Consulte 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 canalización de CI/CD puede utilizar varios repositorios.

caché en frío

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

datos fríos

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

visión artificial (CV)

Campo de la IA que utiliza el 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, compilación, 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 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.

defense-in-depth

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

administrador delegado

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

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

Implementación

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

entorno de desarrollo

Consulte entorno.

control de detección

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

asignación de flujos de valor para el desarrollo (DVSM)

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

gemelo digital

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

tabla de dimensiones

En un esquema en estrella, tabla más pequeña que contiene los atributos de datos sobre los datos cuantitativos 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 ante desastres de cargas de trabajo en AWS: Recovery in the Cloud in the AWS Well-Architected Framework.

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. Este concepto lo introdujo Eric Evans en su libro, Diseño impulsado por el dominio: abordando la complejidad en el corazón del software (Boston: Addison-Wesley Professional, 2003). Para obtener información sobre cómo utilizar el diseño basado en dominios con el patrón de higos estranguladores, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

DR

Consulte recuperación ante desastres.

Detección de 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. Los sistemas big-endianos almacenan primero el byte más significativo. Los sistemas Little-Endian 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 AWS PrivateLink y conceder permisos a otros Cuentas de AWS o a responsables AWS Identity and Access Management (de IAM). Estas cuentas o

entidades principales pueden conectarse a su servicio de punto de conexión de forma privada mediante la creación de puntos de conexión de VPC de interfaz. Para obtener más información, consulte Creación de un servicio de punto de conexión en la documentación de Amazon Virtual Private Cloud (Amazon VPC).

planificación de recursos empresariales (ERP)

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, mediante el que los modelos aprenden a partir de ejemplos (pasos) incrustados en las peticiones. La técnica de peticiones con pocos pasos puede ser eficaz para las 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)

Una gran red neuronal de aprendizaje profundo que se ha estado entrenando con conjuntos de datos masivos de datos generalizados y sin etiquetar. FMs son capaces de realizar una amplia variedad de tareas generales, como comprender el lenguaje, generar texto e imágenes

y conversar en lenguaje natural. Para más información, consulte ¿Qué son los modelos fundacionales?

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 la sección Restringir la distribución geográfica del contenido en la CloudFront documentación.

Flujo de trabajo de Gitflow

Un enfoque en el que los entornos inferiores y superiores utilizan diferentes ramas en un repositorio de código fuente. El flujo de trabajo de Gitflow se considera heredado, 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 el cumplimiento en todas las unidades organizativas (OUs). Las barreras de protección preventivas aplican políticas para garantizar la alineación con los estándares de conformidad. Se implementan mediante políticas de control de servicios y límites de permisos de IAM. Las barreras de protección de detección detectan las vulneraciones de las políticas y los problemas de conformidad, y generan alertas para su corrección. Se implementan mediante Amazon AWS Config AWS Security Hub CSPM GuardDuty AWS Trusted Advisor, Amazon Inspector y AWS Lambda cheques personalizados.

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.

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 de DevOps publicación típico.

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 más información, consulte la práctica recomendada Implementación mediante una infraestructura inmutable en el Marco de 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 AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación y el resto de Internet.

migración gradual

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

Industria 4.0

Término que introdujo Klaus Schwab en 2016 para referirse a la modernización de los procesos de fabricación mediante los avances en la conectividad, los datos en tiempo real, la automatización, el análisis, la IA y el 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 (T) IIo

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

VPC de inspección

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

Internet de las cosas (IoT)

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

interpretabilidad

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

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

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

administración de servicios de TI (ITSM)

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

ITIL

Consulte 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 obtener más información, consulte Qué son. LLMs

migración grande

Migración de 300 servidores o más.

LBAC

Consulte control de acceso basado en etiquetas.

privilegio mínimo

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

migrar mediante lift-and-shift

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 para lo cual 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.

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 Framework.

cuenta de miembro

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

MES

Consulte sistema de ejecución de fabricación.

Message Queuing Telemetry Transport (MQTT)

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

microservicio

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

arquitectura de microservicios

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

Programa de aceleración de la migración (MAP)

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

migración a escala

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

fábrica de migración

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

metadatos de migración

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

patrón de migración

Tarea de migración repetible que detalla la estrategia de migración, el destino de la migración y la aplicación o el servicio de migración utilizados. Ejemplo: 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 fiabilidad y la previsibilidad, el AWS Well-Architected Framework 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.

Open Process Communications: arquitectura unificada (OPC-UA)

Un protocolo de machine-to-machine comunicación (M2M) para la automatización industrial. OPC-UA establece un estándar de interoperabilidad con esquemas de autenticación, autorización y cifrado 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 más información, consulte Operational Readiness Reviews (ORR) en el Marco de AWS Well-Architected.

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 para todos los miembros 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 AWS KMS (SSE-KMS) y las solicitudes dinámicas `PUT` y `DELETE` dirigidas al bucket de S3.

identidad de acceso de origen (OAI)

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

ORR

Consulte 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 AWS de referencia de seguridad recomienda configurar la cuenta de red con entradas, salidas e inspección VPCs para proteger la interfaz bidireccional entre la aplicación e Internet en general.

P

límite de permisos

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

información de identificación personal (PII)

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

PII

Consulte 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

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

control proactivo

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 la sección 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)

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

punto de enlace de servicio

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

acuerdo de nivel de servicio (SLA)

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

indicador de nivel de servicio (SLI)

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

objetivo de nivel de servicio (SLO)

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.

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.

split-and-seed modelo

Un patrón para escalar y acelerar los proyectos de modernización. A medida que se definen las nuevas funciones y los lanzamientos de los productos, el equipo principal se divide para crear nuevos equipos de productos. Esto ayuda a ampliar las capacidades y los servicios de su organización, mejora la productividad de los desarrolladores y apoya la innovación rápida. Para 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 con la aplicación de este patrón, consulte Modernización gradual de los servicios web antiguos de Microsoft ASP.NET (ASMX) mediante contenedores y Amazon API Gateway.

subred

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

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

Pares clave-valor que actúan como metadatos para organizar los recursos. AWS 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.

puerta de enlace de tránsito

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

flujo de trabajo basado en enlaces troncales

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

acceso de confianza

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

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

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

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

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

vulnerabilidad

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

W

caché caliente

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

datos templados

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

función de ventana

Función SQL que 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.