Invertir en la ingeniería del caos como una necesidad estratégica

AWS Guía prescriptiva

AWS Guía prescriptiva: Invertir en la ingeniería del caos como una necesidad estratégica

Table of Contents

Invertir en la ingeniería del caos como una necesidad estratégica

Adrian Hornsby, Amazon Web Services

Enero de 2025 (historial del documento)

Las prácticas de ingeniería del caos utilizan las interrupciones controladas para identificar los problemas y las oportunidades del sistema a fin de evitar interrupciones y otros incidentes. La ingeniería del caos se ha vuelto esencial para mejorar la resiliencia de los sistemas, pero su adopción generalizada se enfrenta a obstáculos relacionados con los conceptos erróneos, la resistencia cultural, los recursos y la forma de cuantificar el valor empresarial. Establecer objetivos iniciales ayuda a poner en marcha los esfuerzos de ingeniería del caos, mientras que cuantificar el retorno de la inversión (ROI) justifica la inversión continua, especialmente en un contexto de presiones económicas.

Este documento de estrategia describe un enfoque holístico para captar tanto las mejoras operativas cuantitativas como los beneficios organizativos cualitativos. El objetivo final es tratar la ingeniería del caos como una necesidad estratégica similar a la ciberseguridad y no como un ejercicio continuo de justificación de costes.

Los costos de inactividad y el surgimiento de la ingeniería del caos

La consultora de inteligencia tecnológica de la información (ITIC) estima que el 90 por ciento de las empresas se enfrentan a costes que superan los 300 000$ por hora de inactividad, y que el 41 por ciento supera los 1 a 5 millones de dólares por hora. Además de la pérdida inmediata de ingresos, el tiempo de inactividad puede provocar problemas a largo plazo, como incumplimientos, bajadas de los precios de las acciones, importantes costes de mitigación e incluso daños a la marca.

Si bien el tiempo de inactividad suele asociarse a los sistemas en línea que generan ingresos, el impacto negativo va mucho más allá. Todas las grandes empresas y organizaciones, independientemente de su modelo de ingresos principal, dependen en gran medida de la disponibilidad de sus sistemas internos, como los de recursos humanos y de nómina.

El tiempo de inactividad que afecta a estos servicios internos básicos puede inhibir la capacidad de funcionamiento de una empresa y provocar importantes interrupciones operativas y repercusiones financieras. Los problemas resultantes pueden incluir los siguientes:

- Retrasos en el pago a los empleados y vendedores
- Incapacidad para procesar los pedidos o transacciones de los clientes
- Los sistemas de seguridad comprometidos permiten filtraciones de datos confidenciales
- Pérdida de productividad y oportunidades de ingresos
- Sanciones reglamentarias en caso de incumplimiento
- Daño a la reputación de la marca

La ingeniería del caos introduce intencionadamente interrupciones controladas. El uso de la ingeniería del caos para comprender o verificar la respuesta del sistema a las deficiencias se ha convertido en una práctica fundamental para mejorar la resiliencia del sistema. La ingeniería del caos permite a su organización descubrir problemas de forma proactiva, validar los mecanismos de resiliencia y, en última instancia, reducir el riesgo de tiempos de inactividad no planificados y los costes asociados. Los beneficios de la ingeniería del caos incluyen los siguientes:

- Revelando la deuda técnica
- Ejercitar los músculos operativos
- Fomentar la confianza en los sistemas

- Identificar los puntos de falla
- Mejorar el monitoreo y la observabilidad
- Apoyar el aprendizaje basado en experimentos
- Ofrecer una mayor resiliencia para reducir el tiempo de inactividad

A medida que los sistemas se vuelven más complejos y aumentan las expectativas de los clientes, la ingeniería del caos adquiere cada vez más importancia. Gartner recomienda la ingeniería del caos como una práctica fundamental para que las organizaciones reduzcan el tiempo de inactividad no planificado y mejoren la resiliencia.

Los desafíos de adopción de la ingeniería del caos

Si bien la ingeniería del caos es una práctica cada vez más importante para mejorar la resiliencia de los sistemas, su adopción puede enfrentarse a los siguientes obstáculos:

- Percepciones erróneas sobre el riesgo: una idea errónea común es que la ingeniería del caos solo se lleva a cabo en entornos de producción, lo que genera preocupación por el riesgo excesivo. Esta percepción se debe a la falta de comprensión sobre la naturaleza sistemática y controlada de las prácticas de ingeniería del caos. Como se indica en el AWS Well-Architected Framework, primero realice la simulación de fallas en un entorno que no sea de producción.
- A largo plazo para el valor empresarial: los beneficios de la ingeniería del caos se acumulan gradualmente, lo que dificulta la cuantificación del valor empresarial y la justificación de la inversión inicial. El menor retorno de la inversión dificulta que las organizaciones prioricen y sigan con la ingeniería del caos.
- Brechas de habilidades y experiencia: la ingeniería del caos requiere un conjunto único de habilidades y conocimientos que tal vez no estén fácilmente disponibles en su organización. Desarrollar o adquirir esta experiencia puede ser un obstáculo importante, especialmente para las organizaciones que son nuevas en esta práctica y aquellas con recursos limitados.

El resto de este documento de estrategia se centrará principalmente en el segundo desafío, que consiste en demostrar el valor empresarial de la ingeniería del caos.

Los efectos acumulativos de la ingeniería del caos

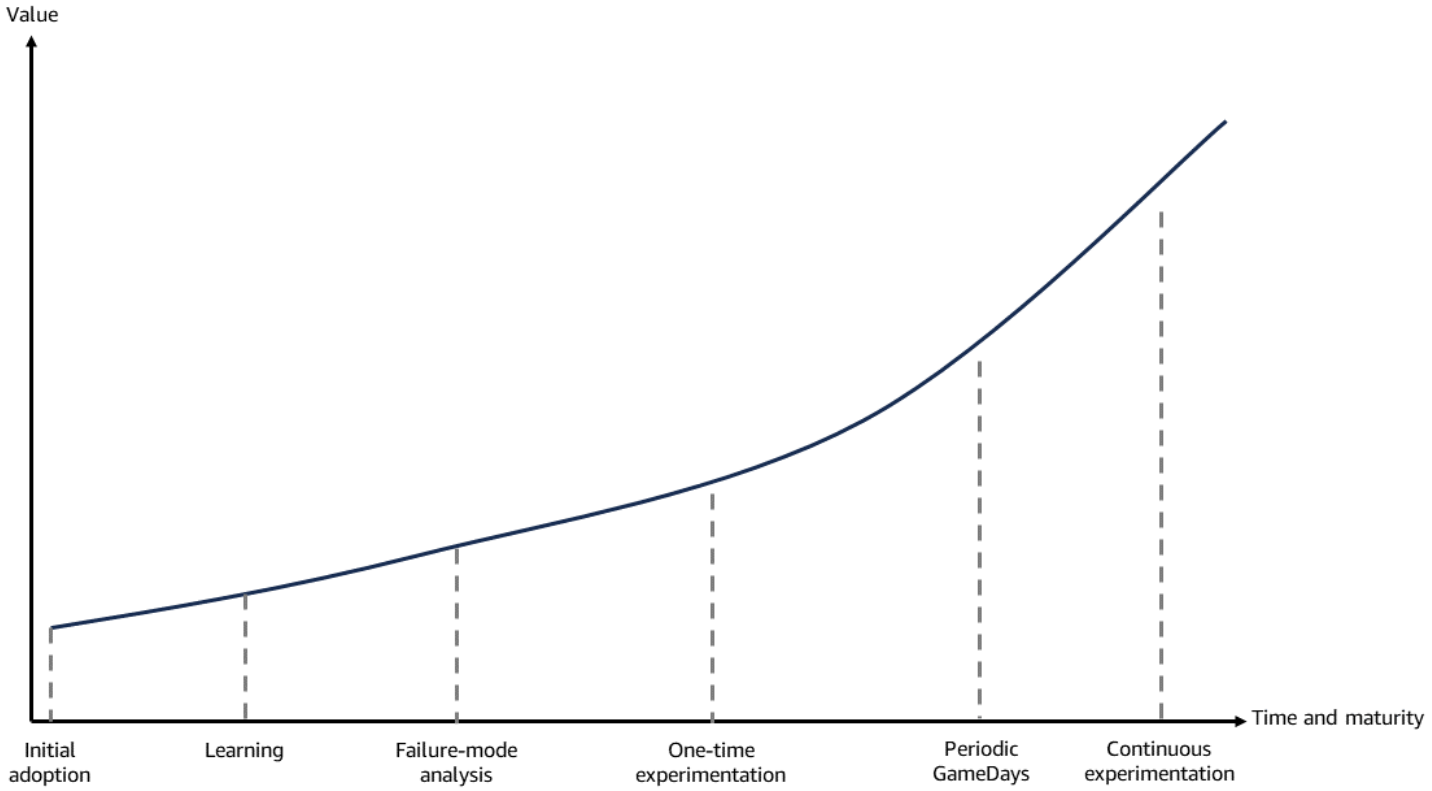
A diferencia de los proyectos tecnológicos tradicionales con fechas de inicio y finalización bien definidas, la ingeniería del caos es una práctica continua de aprendizaje continuo y mejoras continuas en la resiliencia del sistema. Los beneficios de la ingeniería del caos se agravan con el tiempo.

A medida que los sistemas evolucionan y se vuelven más complejos, surgen nuevos modos de falla. Se necesitan más experimentos de caos para identificar posibles problemas. Solucionar un problema puede llevar meses, especialmente en grandes empresas con sistemas y procesos complejos, o cuando los fallos son propiedad de proveedores de servicios externos.

El cambio cultural hacia aceptar el fracaso como una oportunidad de aprendizaje y mejora crece con el paso de los años y se va arraigando en la organización. Las inversiones en la automatización de los experimentos de ingeniería del caos y en el desarrollo de herramientas de apoyo siguen agilizando y mejorando la práctica de la ingeniería del caos. Desarrollar este conocimiento institucional y comprender la resiliencia del sistema es un proceso gradual que se acumula con el tiempo. El conocimiento, los procesos y las herramientas desarrollados a través de la ingeniería del caos aumentan de valor a medida que la práctica madura junto con los sistemas en continua evolución.

El siguiente diagrama muestra cómo el valor aumenta con el tiempo a medida que la adopción del caos avanza en las siguientes etapas:

- Adopción inicial
- Aprendizaje
- Análisis del modo de falla
- Experimentos únicos
- Periódico GameDays
- Experimentación continua



Como se muestra en el diagrama, los beneficios de la ingeniería del caos suelen empezar antes de que se produzca una avería en el sistema. El proceso de planificación y diseño de los experimentos de caos en sí mismo proporciona un valor inmediato. La identificación de posibles escenarios de falla, puntos únicos de falla y áreas de incertidumbre en el sistema conduce a mejoras.

Por ejemplo, anotar los escenarios de falla y analizar los posibles efectos en cascada, un proceso denominado análisis del modo y los efectos de las fallas (FMEA), ayuda a descubrir debilidades o brechas obvias que podrían haberse pasado por alto. Su organización puede abordar estos problemas de forma proactiva, incluso antes de que el sistema sufra interrupciones intencionadas. Para obtener más información, consulte el marco de análisis de resiliencia.

Además, el mayor enfoque en la observabilidad y el monitoreo del sistema, que suele acompañar a las iniciativas de ingeniería del caos, comienza a generar beneficios de inmediato. Mejorar la visibilidad del comportamiento del sistema y de los modos de fallo ayuda al equipo a comprender mejor las condiciones normales de funcionamiento del sistema. Una mayor visibilidad también ayuda al equipo a comprender cómo las condiciones de operación se degradan, se adaptan y fallan cuando se las lleva al límite.

Tanto el modo de experimento único como el GameDay modo periódico son enfoques más manuales en comparación con el modo de experimentación continua. Requieren un proceso más práctico y

exploratorio, en el que los ingenieros diseñan y perfeccionan activamente las hipótesis a través de sus observaciones y experimentos.

El modo de experimentación continua es, por otro lado, de naturaleza más automatizada. Este modo se centra en ejecutar hipótesis aprobadas y validadas de forma controlada e iterativa. Utiliza la automatización y la integración en el proceso de desarrollo a través de un proceso de creación de caos específico para garantizar que los experimentos sean coherentes y repetibles.

Iniciativas populares de ingeniería del caos

El camino de la ingeniería del caos a menudo comienza a nivel de base, donde los equipos de ingeniería identifican las necesidades y comienzan a experimentar con la ingeniería del caos de forma independiente.

En este enfoque de base, los equipos experimentan, aprenden y perfeccionan sus prácticas de ingeniería del caos. El valor de la ingeniería del caos se puede demostrar a través de los siguientes resultados tangibles:

- Reducción de incidentes
- Mejor observabilidad
- Tiempos de recuperación más rápidos
- Resiliencia del sistema mejorada y continua

Las iniciativas populares de ingeniería del caos suelen surgir en condiciones organizativas específicas. Requieren un entorno con un alto grado de autonomía de ingeniería, en el que los equipos tengan la libertad de experimentar e innovar sin barreras burocráticas excesivas. La experiencia local en ingeniería de resiliencia o sistemas distribuidos es crucial, porque proporciona la base técnica para comprender e implementar los experimentos de caos. Y lo que es más importante, estas iniciativas suelen apoyarse en los defensores del caos, personas apasionadas que entienden el valor de la ingeniería del caos. Los campeones del caos están dispuestos a abogar por la adopción de la ingeniería del caos, formar a sus colegas e impulsar los primeros experimentos. Sin libertad organizativa, experiencia técnica y defensores motivados, los esfuerzos de base en la ingeniería del caos rara vez se arraigan, independientemente de sus posibles beneficios.

El papel de los objetivos en la adopción de la ingeniería del caos

Es habitual que los objetivos iniciales surjan de forma orgánica a partir de los esfuerzos de base para crear el caos dentro de una organización. Impulsados por la necesidad de abordar sus propios problemas recurrentes, estos equipos o grupos suelen explorar prácticas de ingeniería del caos sin la aprobación explícita ni el establecimiento de prioridades por parte de los niveles superiores.

Los equipos pueden utilizar estos resultados para presentar argumentos convincentes a favor de una adopción más amplia por parte de la organización y, de este modo, convertirse en un campo de pruebas para otros equipos.

Cuando los beneficios de los esfuerzos de base se vuelven demasiado importantes como para ignorarlos, estos equipos pueden convertir sus esfuerzos y conocimientos en liderazgo y establecer metas. Esta mayor visibilidad puede facilitar la adopción de objetivos de resiliencia en toda la organización y generar el apoyo y los recursos necesarios para implementar la ingeniería del caos.

Los objetivos, en particular los impulsados por los líderes y establecidos en respuesta a interrupciones importantes, desempeñan un papel crucial a la hora de catalizar la adopción de prácticas de ingeniería del caos. Entre los tipos de objetivos más comunes se incluyen los siguientes:

- Objetivos de disponibilidad para identificar y reducir los puntos únicos de fallo (SPOF)
- Objetivos de recuperación del servicio para mejorar la capacidad de recuperación en caso de interrupciones o fallas
- Objetivos de experiencia de usuario para cumplir objetivos específicos de nivel de servicio () SLOs
- Objetivos basados en métricas para hacer un seguimiento del progreso en la mitigación de los riesgos de disponibilidad conocidos y la implementación de las medidas de resiliencia recomendadas
- Objetivos normativos y de cumplimiento para demostrar la resiliencia operativa

Para obtener más información sobre algunos de estos tipos de objetivos y sobre cómo Amazon y otras organizaciones los han utilizado durante la adopción de la ingeniería del caos, consulta el Apéndice A.

Estos objetivos sirven como una justificación convincente y proporcionan un enfoque específico y práctico para impulsar la adopción de la ingeniería del caos. Al principio, los objetivos sirven como

indicador de las métricas de ROI tradicionales. Los objetivos ofrecen una razón convincente cuando los cálculos cuantificables del ROI sobre la resiliencia pueden resultar difíciles de obtener. Si no se adoptan estos objetivos en una fase temprana, la práctica de la ingeniería del caos corre el riesgo de no demostrar su eficacia y de lograr una aceptación más amplia de la organización.

El cambio de los objetivos a la medición del ROI

A medida que las prácticas van madurando y se van alcanzando los objetivos iniciales, el enfoque pasa de centrarse en establecer objetivos a cuantificar los beneficios financieros tangibles de la ingeniería del caos: el retorno de la inversión (ROI). El cambio se debe a dos razones principales:

- Consideraciones económicas
- Preservar la experiencia y la confianza del cliente

Consideraciones económicas

En tiempos de crecimiento económico y finanzas saneadas, las empresas no suelen necesitar una justificación exhaustiva para establecer objetivos específicos en sus estrategias de ingeniería del caos. Sin embargo, los cambios en el panorama financiero han llevado a muchas organizaciones a reevaluar sus inversiones, y las implementaciones de ingeniería caótica deben proporcionar un ROI cuantificado.

Estas empresas ahora tienen la tarea de establecer métricas de ROI claras y tradicionales para demostrar el valor y el impacto de las prácticas de ingeniería del caos. Este desafío se complica aún más por la paradoja de la prevención. La paradoja de la prevención se produce cuando la prevención exitosa de los incidentes dificulta la justificación de la inversión, ya que las partes interesadas tienden a infravalorar las catástrofes evitadas. Incluso las organizaciones con una cultura de excelencia operativa profundamente arraigada se enfrentan a la presión de utilizar las métricas del ROI para justificar la adopción continua de la ingeniería del caos.

Preservar la experiencia y la confianza de los clientes

Mantener una resiliencia impulsada por los objetivos puede ser un desafío a largo plazo. Una vez que se alcanza un objetivo inicial, como alcanzar un objetivo de tiempo de recuperación, resulta difícil justificar una inversión continua en ingeniería del caos hasta que se produzca una próxima interrupción importante. El flujo y el reflujo de la inversión crean un ciclo reactivo en forma de diente de sierra. Con cada nueva interrupción, la inversión en resiliencia aumenta con un nuevo objetivo que aborda la causa fundamental. Una vez alcanzado el nuevo objetivo, la inversión cae hasta el siguiente incidente, lo que reinicia el ciclo reactivo.

Las interrupciones que impulsan este enfoque reactivo tienen un impacto negativo en los clientes. La pregunta clave: ¿cuántas interrupciones importantes tolerarán los clientes antes de abandonar un proveedor de servicios en favor de un competidor más resiliente?

Cuantificación del ROI de la ingeniería del caos

En la actualidad, muy pocos recursos publicados proporcionan metodologías completas o datos del mundo real para cuantificar el retorno de la inversión (ROI) a largo plazo de la ingeniería del caos.

En el paper The Business Case for Chaos Engineering, Netflix ofrece una valiosa ecuación para calcular el ROI de la ingeniería del caos. Esta ecuación proporciona un punto de partida para las organizaciones que se embarcan en su viaje hacia la ingeniería del caos.

La ecuación requiere que calcule con precisión los costos de lo siguiente:

- Interrupciones evitables y no evitables
- Costos de implementación del programa de ingeniería del caos
- Costos de los daños inducidos por el caos

El daño provocado por el caos se refiere al impacto negativo o la perturbación que se produce al inyectar deliberadamente fallas o condiciones turbulentas en un sistema como parte de los experimentos de ingeniería del caos. La ecuación requiere estimar los costos de las interrupciones evitables y no evitables, los costos de implementación de los programas de ingeniería del caos y los costos de los daños provocados por el caos.

Determinar con certeza qué problemas podrían haberse evitado con un programa de ingeniería del caos es una tarea difícil. Requiere un análisis hipotético que implique analizar las causas fundamentales de los problemas y especular sobre cómo los experimentos de ingeniería del caos podrían haber ayudado a identificarlos. Este análisis es difícil porque los sistemas modernos son muy complejos y presentan numerosas interdependencias e interacciones entre varios componentes, servicios y bibliotecas de terceros. Además, las fallas en los sistemas suelen ser no deterministas y, en retrospectiva, las condiciones que las provocan pueden resultar difíciles de entender completamente.

Si bien el enfoque sugerido por Netflix tiene algunas limitaciones, constituye una buena base para las organizaciones que comienzan a explorar la ingeniería del caos. La ecuación puede guiarlo a la hora de estimar los costos y los beneficios potenciales, lo que le ayudará a tomar decisiones sobre la implementación de un programa de este tipo. Sin embargo, a medida que las organizaciones avanzan en su camino hacia la ingeniería del caos, es importante ampliar la evaluación del ROI para incorporar una perspectiva más holística.

Este enfoque holístico no solo capturará los beneficios directos de la reducción de las interrupciones y los costos de ingeniería, sino que también destacará los efectos transformadores a largo plazo en la resiliencia general de la organización. Captura los beneficios acumulados y los efectos organizacionales más amplios de la ingeniería del caos para ofrecer una representación más precisa del verdadero valor y el impacto de la ingeniería del caos.

Un enfoque holístico para la cuantificación del ROI

Una evaluación holística del ROI debe tener en cuenta no solo las medidas cuantitativas sino también los factores cualitativos. El enfoque holístico requiere datos del mundo real de organizaciones que practican la ingeniería del caos a gran escala durante períodos de tiempo más largos. Puede utilizar los datos partiendo de los proyectos y objetivos básicos y pasando por cualquier dato de ROI que haya recopilado con un enfoque de ecuaciones.

Las medidas cuantitativas se centran en las cantidades o frecuencias. Las mediciones son objetivas y se pueden analizar estadísticamente. Los ejemplos incluyen encuestas, experimentos y análisis de datos. Las medidas cuantitativas pueden incluir lo siguiente:

- Métricas de incidentes
- Costos
- Mejoras
- Conformidad
- Tasas de adopción
- Satisfacción del cliente

El seguimiento de las medidas cuantitativas puede demostrar los beneficios operativos directos de la ingeniería del caos.

Las medidas cualitativas son descriptivas y se centran en comprender las experiencias y las opiniones. A menudo son subjetivas y no se pueden medir numéricamente fácilmente. En el caso de la ingeniería del caos, las medidas cualitativas capturan los impactos organizacionales más amplios. Las medidas cualitativas pueden incluir lo siguiente:

- Confianza de los empleados
- Cambio cultural
- Colaboración

- Efectividad de la formación
- Retención del talento
- Reputación de marca
- Ventaja competitiva

Al tener en cuenta tanto los impactos financieros cuantitativos como los beneficios organizacionales cualitativos, puede tomar decisiones más informadas sobre la inversión continua en la ingeniería del caos y, al mismo tiempo, fomentar una cultura de resiliencia.

Para obtener más información sobre estas medidas y su marco de clasificación de incidentes asociado, consulte los apéndices B y C.

La transición del ROI a la ingeniería del caos como una necesidad estratégica

Si bien resulta tentador monitorizar el ROI, los desafíos que supone medir el valor de la ingeniería del caos suelen llevar a las organizaciones a priorizar la eficiencia inmediata y a corto plazo por encima de las inversiones en resiliencia estratégica. Este enfoque pasa por alto la ingeniería del caos como un factor clave de la resiliencia y las ventajas competitivas de evitar las interrupciones. El verdadero valor de la ingeniería del caos reside en prevenir futuros fracasos. La ingeniería del caos apoya la continuidad empresarial a largo plazo.

En lugar de centrarse en el ROI, trate la ingeniería del caos como ciberseguridad. Como se explica en el artículo de Forbes La ciberseguridad como inversión estratégica: cómo la optimización del ROI puede conducir a un futuro más seguro, la ciberseguridad no debe considerarse un centro de costes o un gasto obligatorio para las organizaciones, ya que esa mentalidad no reconoce el valor estratégico que las medidas sólidas de ciberseguridad pueden aportar a lo largo del tiempo. En cambio, el autor sostiene que al cambiar las perspectivas para tratar la ciberseguridad como una inversión a largo plazo que genera ventajas competitivas, las organizaciones pueden abrir nuevas vías para la innovación, la eficiencia operativa y la diferenciación dentro de sus respectivos mercados. Al adoptar este enfoque, el autor concluye que los directores de seguridad de la información (CISOs) pueden garantizar mejor la aceptación y la financiación de los líderes. De este modo, pueden posicionar a sus empresas para superar a sus competidores en un panorama cibernético cada vez más riesgoso. Esta creación de valor estratégico y a largo plazo de la ciberseguridad es paralela a las mejoras continuas inherentes a las prácticas de ingeniería del caos.

Mientras que la seguridad salvaguarda la capacidad de una organización para operar y proteger los activos, la ingeniería del caos ayuda a garantizar la disponibilidad, la confiabilidad y la capacidad de recuperación de los sistemas y servicios principales. Para obtener valor a largo plazo y obtener una ventaja competitiva, considere la ingeniería del caos como una capacidad fundamental y un imperativo estratégico, no como una iniciativa que requiere una justificación constante.

El siguiente diagrama muestra la evolución de la ingeniería del caos, que ha pasado de ser algo básico a convertirse en objetivos y retorno de la inversión (ROI), para convertirse en una estrategia.

A nivel de base, los equipos individuales suelen experimentar de forma independiente, impulsados por las necesidades locales. Estos experimentos están respaldados por ingenieros apasionados que demuestran su valor mediante la reducción de los incidentes y la mejora de la observabilidad.

Cuando estos esfuerzos tienen éxito, los equipos pueden convertir su aprendizaje en liderazgo. Con esta visibilidad, los esfuerzos pasan a una fase basada en objetivos. La organización establece objetivos formales para la resiliencia y la recuperación, respaldados por recursos y apoyo para una implementación más amplia.

Por último, la ingeniería del caos va más allá de la necesidad constante de justificar el ROI para convertirse en una necesidad estratégica, similar a la ciberseguridad. En esta etapa, la ingeniería del caos se integra completamente en los procesos organizacionales. La implementación se centra en la resiliencia a largo plazo más que en las métricas a corto plazo. La ingeniería del caos se considera una capacidad fundamental esencial para mantener la ventaja competitiva y la confianza de los clientes.

Integrar la ingeniería del caos en su organización

Para llevar la ingeniería del caos al mismo nivel de importancia que la seguridad, tenga en cuenta las siguientes sugerencias:

- Establezca la ingeniería del caos como una práctica innegociable: del mismo modo que la ciberseguridad se considera un requisito fundamental para las organizaciones, considérela como una práctica obligatoria para garantizar la resiliencia y la fiabilidad del sistema. Integre la ingeniería del caos en los procesos, las herramientas y la cultura de su organización, en lugar de considerarla una actividad opcional o discrecional. Para obtener más información, consulte la guía del marco del ciclo de vida de la resiliencia.
- Garantice la aceptación y el apoyo de los ejecutivos: al igual que ocurre con las iniciativas de seguridad, las iniciativas de ingeniería del caos deben contar con la aceptación y el apoyo activo de los líderes ejecutivos. Esto incluye asignar recursos, presupuesto y personal dedicados a implementar y mantener las prácticas de ingeniería del caos en toda la organización.

- Implemente la gobernanza y la supervisión: de forma similar a un marco de CISO y gobernanza de la seguridad, establezca un equipo especializado en ingeniería del caos o un director de resiliencia. Este equipo o función es responsable de supervisar y coordinar las iniciativas de ingeniería del caos en los diferentes equipos y unidades de negocio.
- Integre la ingeniería del caos en los ciclos de desarrollo y operaciones: del mismo modo que las prácticas de seguridad se integran en los procesos de desarrollo e implementación del software, convierta la ingeniería del caos en una parte integral del ciclo de vida de desarrollo y entrega del software.
- Realice simulaciones y simulacros de ingeniería del caos con regularidad. Al igual que en las simulaciones de brechas de seguridad y los simulacros de respuesta a incidentes, realice experimentos periódicos de ingeniería del caos para validar las capacidades de respuesta a incidentes e identificar los posibles puntos ciegos de forma proactiva.
- Utilice la ingeniería del caos para mantener los manuales de ejecución: al igual que ocurre con la realización de revisiones de seguridad, utilice experimentos de ingeniería del caos para validar la eficacia y precisión de los manuales de ejecución a la hora de responder a los incidentes y recuperarse de ellos. Además, los experimentos de ingeniería del caos pueden servir como simulaciones realistas para que los ingenieros de guardia practiquen la ejecución de procedimientos manuales. Las simulaciones ayudan a los ingenieros a mantener su capacidad de memoria operativa y a estar preparados para hacer frente a los incidentes del mundo real.
- Fomente una cultura de resiliencia: al igual que ocurre con la formación en materia de concienciación sobre la seguridad, invierta en la educación en ingeniería del caos y en iniciativas de intercambio de conocimientos para fomentar una cultura de resiliencia. Incluya programas de formación, colaboración interfuncional e incentivos para los equipos que adopten prácticas de ingeniería del caos.
- Mida las métricas de resiliencia e informe al respecto: supervise periódicamente las métricas de resiliencia e infórmelas a las partes interesadas. Utilice las métricas cuantitativas y cualitativas analizadas en este documento como punto de partida.
- Considere la resiliencia como una ventaja competitiva: las medidas de ciberseguridad pueden proporcionar una ventaja competitiva. Del mismo modo, considere sus capacidades de ingeniería del caos y resiliencia como un elemento diferenciador que le ayude a ofrecer servicios más fiables y dignos de confianza a sus clientes.

Conseguir la aceptación de los ejecutivos

La ingeniería del caos a menudo carece de un responsable claro dentro de las responsabilidades tradicionales de la alta dirección. El CEO se preocupa por el crecimiento, la rentabilidad y el liderazgo en el mercado. El CFO se centra en el rendimiento financiero, el control de costes y la gestión de riesgos. El CTO prioriza la estrategia tecnológica, las hojas de ruta de los productos y la excelencia en ingeniería. El CISO supervisa la seguridad y el cumplimiento.

Dado que ningún ejecutivo es realmente dueño de la resiliencia, a menudo es difícil conseguir la aceptación y el apoyo. Sin embargo, las fallas del sistema afectan a los ingresos, la satisfacción de los clientes y la reputación de la marca, algo que preocupa al CEO y al CFO. El CTO y el CISO tienen la tarea de implementar medidas de resiliencia, pero es posible que carezcan de un mandato organizacional. Esta ambigüedad puede impedir la realización de inversiones estratégicas y la alineación de la organización hacia una estrategia de resiliencia común.

Esta ambigüedad también dificulta que los ejecutivos acepten las iniciativas de resiliencia, como la ingeniería del caos. Al fin y al cabo, los líderes de alto nivel están haciendo malabares con una multitud de prioridades estratégicas: crecimiento, innovación, experiencia del cliente, cumplimiento y más.

Para comunicar de manera efectiva el valor de la ingeniería del caos a los ejecutivos de alto nivel, considere los siguientes enfoques:

- Determine las principales preocupaciones y los factores que impulsan la toma de decisiones de sus ejecutivos de alto nivel.

  Por ejemplo, ¿los altos ejecutivos están preocupados por la pérdida de clientes, el cumplimiento de las normas, la reducción de costes o las presiones competitivas? Posicione la ingeniería del caos como un multiplicador de fuerzas que se alinee con los desafíos y objetivos únicos de la empresa.
- Identifique los objetivos compartidos y los resultados estratégicos.

  ¿Cómo apoya su estrategia de ingeniería del caos la estrategia general de crecimiento de la organización, la experiencia del cliente, las oportunidades de mercado y la eficiencia operativa? Priorice las iniciativas en función de los objetivos, el impacto empresarial, el ROI y el riesgo de no llevarlas a cabo.
- Comunique la eficacia de su estrategia de ingeniería del caos en términos cuantificables mediante el uso de indicadores clave de resiliencia.

Comience con estos cuatro indicadores clave de resiliencia: disponibilidad, tiempo de detección, tiempo de respuesta y tiempo de recuperación. Combínelos directamente con los resultados empresariales, como los ingresos, el ahorro de costes y la reputación de la marca.

- No se pierda en los detalles técnicos.

  Céntrese en la opinión general y en el impacto empresarial medible. La alta dirección se preocupa por los resultados que impulsan el crecimiento, aumentan la confianza de los clientes y fomentan la innovación.

La paradoja de la prevención

Cuando las fallas se mitigan con éxito antes de que se manifiesten, resulta difícil convencer a las partes interesadas del valor y la necesidad de las medidas preventivas adoptadas. Este fenómeno se conoce como la paradoja de la prevención. La paradoja de la prevención es el mayor obstáculo para integrar la ingeniería del caos como una necesidad estratégica, y se debe a los sesgos inherentes a la cognición humana.

El error del año 2000 ilustra muy bien esta paradoja. Se invirtieron años de preparación y miles de millones de dólares en la actualización de los sistemas informáticos en todo el mundo. Sin embargo, muchos interpretaron la transición sin contratiempos al año 2000 como una prueba del carácter exagerado de las preocupaciones relacionadas con el año 2000. Pocas veces se reconoció el éxito de los esfuerzos preventivos emprendidos.

Esta paradoja de la prevención sigue siendo un desafío para las organizaciones que hoy en día invierten en la ingeniería del caos. Cuando las posibles interrupciones se evitan con éxito mediante medidas proactivas, la mera ausencia de una catástrofe puede, paradójicamente, dificultar la justificación de los recursos que se gastan en la prevención.

La causa fundamental de este fenómeno radica en la forma en que nuestras mentes están programadas para procesar la información. Los procesos cognitivos humanos están orientados a responder y recordar eventos reales y resultados visibles. Cuando se evita un desastre, no hay una narrativa dramática que conservar o compartir. Otro aspecto de la paradoja de la prevención es el sesgo retrospectivo. Cuando no ocurre nada, las personas tienden a llegar a la conclusión de que no pasó nada, por lo que no fue un problema real. No se reconoce la posibilidad de que las precauciones adecuadas evitaran un problema real. Este punto ciego psicológico crea un desafío permanente para las organizaciones. Cuanto más éxito tenga en materia de prevención y resiliencia, más innecesarios serán sus esfuerzos en retrospectiva.

Para abordar la paradoja de la prevención, su organización puede tomar medidas específicas para hacer que la invisible labor de prevención sea visible, mensurable y valorada. Entre las posibles medidas se incluyen las siguientes:

- Documente y simule lo que podría haber sucedido sin medidas preventivas.
- Comparta historias de eventos en los que las medidas preventivas evitaron posibles desastres.
- Indique las organizaciones homólogas que no se prepararon y que, como resultado, sufrieron las consecuencias.
- Presente los costos de la prevención en el contexto de los posibles impactos que están previniendo.
- Divida los esfuerzos de prevención en hitos y logros visibles.
- Construya una memoria institucional sobre por qué existen las medidas preventivas y su importancia histórica.
- Eduque periódicamente a las partes interesadas sobre el valor de las prácticas de ingeniería de la resiliencia y el caos.

Conclusión

La ingeniería del caos es un imperativo estratégico para las organizaciones. Si bien su proceso de adopción puede enfrentarse a desafíos como ideas erróneas, resistencias culturales y limitaciones de recursos, establecer objetivos claros e impulsados por el liderazgo puede catalizar el proceso. A medida que vayan madurando las prácticas, cuantifique el retorno de la inversión mediante un enfoque holístico que refleje tanto las mejoras operativas cuantitativas como los beneficios organizativos cualitativos. El enfoque holístico es especialmente importante durante las presiones económicas.

Para transformar esta necesidad estratégica en realidad, comience por evaluar el nivel de madurez actual de su organización. ¿Se encuentra su organización en la fase de experimentación de base, en la fase orientada a objetivos o en algún punto intermedio? Sobre la base de esta evaluación, cree una hoja de ruta personalizada para lograr lo siguiente:

- Establezca un gobierno de ingeniería del caos (por ejemplo, designe a un director de resiliencia).
- Integre las prácticas de caos en los flujos de trabajo de desarrollo.
- Implemente programas de formación periódicos.
- Desarrolle métricas de resiliencia integrales.

Esta transformación no se producirá de la noche a la mañana. Sin embargo, tomar estas medidas concretas y, al mismo tiempo, garantizar el apoyo ejecutivo continuo, ayudará a llevar la ingeniería del caos al mismo nivel estratégico que la ciberseguridad. Al igual que la ciberseguridad, la ingeniería del caos puede convertirse en una parte integral del ADN y los procesos operativos de su organización.

Recursos

- Resultados de la encuesta mundial sobre hardware y sistema operativo de servidores de la ITIC 2021
- El argumento empresarial a favor de Chaos Engineering
- La ciberseguridad como inversión estratégica: cómo la optimización del ROI puede conducir a un futuro más seguro
- La guía de ingeniería del caos para líderes de I&O
- ¿Cómo utilizar la puntuación de AWS Resilience Hub
- Implementación de los experimentos recomendados mediante la consola AWS Resilience Hub

Apéndice A – Tipos de objetivos para la ingeniería del caos

Las siguientes descripciones de los tipos de objetivos incluyen ejemplos reales de cómo Amazon y otras organizaciones han diseñado objetivos para la ingeniería del caos.

Objetivos de arquitectura resiliente

Uno de los factores iniciales para adoptar la ingeniería del caos es identificar y reducir los puntos únicos de falla (SPOF) en los sistemas y la infraestructura. Los objetivos se establecen para validar la resiliencia de los sistemas y arquitecturas críticos, especialmente en el caso de los nuevos servicios o aplicaciones.

Los objetivos de una arquitectura resiliente implican realizar experimentos caóticos que simulen fallos en las dependencias de los servicios. Los experimentos confirman si los tiempos de espera, los reintentos, el comportamiento del almacenamiento en caché y las configuraciones de los disyuntores funcionan correctamente. Estos experimentos ayudan a descubrir problemas que deben solucionarse y evitar que los incidentes afecten a los clientes. Para ver un ejemplo, consulte Cómo crear servicios resilientes en Prime Video con la ingeniería del caos.

Objetivos de recuperación del servicio

Los objetivos de recuperación del servicio se centran en mejorar la capacidad de recuperación ante las interrupciones operativas o los fallos de la infraestructura. Por ejemplo, su organización podría aspirar a alcanzar un objetivo de tiempo de recuperación (RTO) específico para sus servicios principales en caso de que se produzca una interrupción. Los equipos pueden diseñar experimentos de caos para validar y optimizar las estrategias de evacuación, los mecanismos de conmutación por error y los procesos de recuperación automatizados. En última instancia, las optimizaciones reducen el tiempo necesario para la restauración del servicio. Para ver un ejemplo, consulte AWS Lambda: Resiliencia under-the-hood.

Objetivos de experiencia de usuario

Mantener una experiencia de usuario coherente y fiable es fundamental, especialmente durante los períodos de alto tráfico o los eventos críticos. En esos casos, establezca metas centradas en el cumplimiento de objetivos específicos de nivel de servicio (). SLOs Este enfoque centrado en el cliente garantiza que los esfuerzos de resiliencia estén directamente alineados con la prestación

de una experiencia de usuario superior, incluso ante fallos o condiciones degradantes. Para ver un ejemplo, consulte Resiliencia en ingeniería: lecciones del viaje de Amazon Search a la ingeniería del caos.

Objetivos basados en métricas

Puede establecer objetivos en función de métricas cuantitativas, como una puntuación de resiliencia que se calcula mediante la concesión de puntos a los servicios que adoptan las mejores prácticas de resiliencia comprobadas. A continuación, puede utilizar determinados experimentos de caos para determinar la puntuación de resiliencia. Esta puntuación puede servir como medida para que los equipos hagan un seguimiento de sus avances en la mitigación de los riesgos de disponibilidad conocidos y en la implementación de las medidas de resiliencia recomendadas. Sin embargo, es fundamental interpretar estas puntuaciones con cautela y evitar hacer demasiado hincapié en una sola métrica en detrimento de objetivos de resiliencia más amplios. Para ver un ejemplo, consulte Comprender las puntuaciones de resiliencia.

Objetivos de cumplimiento normativo

El sector de los servicios financieros se ha convertido en uno de los primeros en adoptar la ingeniería del caos, impulsada principalmente por los estrictos requisitos reglamentarios que exigen sólidas capacidades de resiliencia. La normativa exigirá que las instituciones financieras identifiquen, prueben y corrijan de forma proactiva las vulnerabilidades de sus sistemas y procesos críticos. Entre estas normas se incluyen las siguientes:

- El documento interinstitucional sobre prácticas sólidas para fortalecer la resiliencia operativa publicado por las agencias federales de EE. UU.
- Las directrices del Banco Central Europeo sobre la resiliencia operativa
- La propuesta de la Comisión Europea para una Ley de Resiliencia Operativa Digital (DORA)

Si su organización es una institución financiera, cumpla con estas normas estableciendo objetivos explícitos para demostrar la resiliencia operativa mediante estrategias integrales de pruebas y validación. Para ver un ejemplo, consulte El Grupo de la Bolsa de Valores de Londres utiliza la ingeniería del caos AWS para mejorar la resiliencia.

Apéndice B: Medidas cuantitativas y cualitativas

En esta sección se describen las métricas cuantitativas para hacer un seguimiento de las mejoras operativas y las medidas cualitativas para evaluar los resultados organizacionales más amplios derivados de las prácticas de ingeniería del caos.

Medidas cuantitativas

Las siguientes medidas cuantitativas proporcionan un marco para el seguimiento de las métricas clave que pueden demostrar las mejoras operativas y relacionadas con los incidentes directos logradas mediante las prácticas de ingeniería del caos:

- Incidentes:
  - Frecuencia de incidentes: haga un seguimiento del número de incidentes dentro de un marco de clasificación de incidentes y clasifíquelos según su gravedad (crítica, grave o menor) durante un período de tiempo. Para obtener más información sobre el marco de clasificación de incidentes, consulte el apéndice C.
  - Tiempo de inactividad y degradación: mida la duración total del tiempo de inactividad o la degradación del servicio para cada clasificación de incidentes.
  - Métricas de respuesta a los incidentes: para comprender los incidentes, mida el tiempo de detección, el tiempo de identificación, el tiempo de mitigación, el tiempo de recuperación, el tiempo de escalada y otras métricas relacionadas para la clasificación de cada incidente.
  - Incidentes que afectan a los clientes: haga un seguimiento del número de incidentes que afectan a los clientes o del porcentaje de incidentes que se contuvieron antes de que se produjera el impacto en los clientes.
  - Cambios en el manual: realice un seguimiento del número de actualizaciones o revisiones del manual que resultan de la información obtenida a través de experimentos caóticos. Un manual proporciona instrucciones detalladas para realizar una operación o procedimiento en particular para recuperarse de un tipo de incidente en particular.
- Costos:
  - Costos de infraestructura: recopile datos sobre los costos de infraestructura, incluidos los recursos de computación en la nube y las medidas de redundancia que requieren las medidas adoptadas para mejorar la resiliencia.
  - Impacto en los clientes: mida los impactos en la experiencia del cliente, las tasas de abandono y la pérdida de ingresos asociados con los fallos del sistema o el tiempo de inactividad.

    - Productividad del personal: realice un seguimiento del tiempo que los equipos de ingeniería y operaciones dedican a la respuesta a incidentes, la extinción de incendios, la redacción de autopsias y otras tareas reactivas relacionadas con los fallos del sistema.
- Mejoras continuas del sistema: contabilice el número de mejoras en los procesos, cambios en la arquitectura o mecanismos de recuperación automatizados que se han implementado como resultado directo de la información obtenida a partir de experimentos de caos.
- Cumplimiento: realice un seguimiento de los costos y trabaje para cumplir con los requisitos reglamentarios o los estándares del sector relacionados con la resiliencia operativa.
- Adopción: realice un seguimiento de la tasa de adopción de prácticas caóticas en toda la organización.
- Satisfacción del cliente: mida los cambios en las métricas de satisfacción de los clientes para evaluar cómo afecta a la empresa la mejora de la confiabilidad del sistema.

Medidas cualitativas

Las siguientes medidas cualitativas proporcionan un marco para hacer un seguimiento de los resultados organizacionales más amplios logrados mediante las prácticas de ingeniería del caos:

- Confianza y preparación de los empleados:
    - Realice encuestas periódicas a los equipos para medir sus niveles de confianza a la hora de gestionar los incidentes del mundo real y su percepción de que están preparados para las rotaciones de guardia.
    - Realice un seguimiento del porcentaje de ingenieros de guardia que han participado en experimentos de caos como parte de su formación.
- Cambio cultural:
    - Evalúe el grado en que la mentalidad de resiliencia ha impregnado la organización mediante encuestas, sesiones de retroalimentación o auditorías.
    - Haz un seguimiento del número de equipos que defienden y defienden activamente las prácticas de ingeniería del caos.
- Colaboración interfuncional e intercambio de conocimientos:
    - Realice un seguimiento de la frecuencia y la asistencia a las sesiones o talleres de intercambio de conocimientos entre equipos relacionados con el aprendizaje de la ingeniería del caos.
    - Realiza un seguimiento del número de iniciativas conjuntas de ingeniería del caos en las que participan varios equipos o departamentos.

- Efectividad de la formación:
  - Evalúe la eficacia de los programas de formación en ingeniería del caos mediante la realización de encuestas o evaluaciones posteriores a la formación.
  - Haga un seguimiento del número de ingenieros que participan en los programas de formación en ingeniería del caos y lea autopsias.
- Atracción y retención de talentos:
  - Evalúe si el programa de ingeniería del caos ayuda a atraer y retener a los mejores talentos de ingeniería al reducir el tiempo y el esfuerzo dedicados a solucionar las interrupciones.
- Reputación de marca:
  - Realice un seguimiento de cualquier cambio en la percepción o la reputación de la marca relacionado con el compromiso demostrado de la organización con la resiliencia operativa.
- Ventaja competitiva:
  - Haga un seguimiento de la ventaja competitiva con respecto a sus homólogos del sector en términos de disponibilidad del sistema.

Apéndice C – Clasificación de incidentes

El seguimiento de los incidentes dentro de un marco de clasificación es crucial porque el marco proporciona una visión holística de los tipos de fallas y los problemas que afectan al sistema. Si su organización realiza un seguimiento de los incidentes solo dentro de una clase, como las fallas de infraestructura, es posible que pierda información y oportunidades de mejora en otras áreas. Al hacer un seguimiento de los incidentes de varias clases, comprenderá mejor la amplia gama de experimentos de caos que se pueden llevar a cabo. Esta perspectiva ayuda a identificar posibles puntos ciegos y permite ampliar el ámbito de la ingeniería, lo que conduce a un sistema más resiliente y tolerante a los fallos.

El marco de clasificación de incidentes sugerido está diseñado para ayudar a categorizar los incidentes en función de su naturaleza y su impacto potencial. Utiliza una clasificación de alto nivel que agrupa los incidentes en ocho categorías principales:

- Problemas de despliegue:
  - Implementaciones fallidas
  - Fallos de reversión
  - Problemas de configuración durante la implementación
- Errores y regresiones de software:
  - Errores funcionales
  - Problemas de integración
  - Problemas de rendimiento
  - Problemas con las cuotas
  - Problemas con el mecanismo de resiliencia (reintentos, tiempos de espera)
  - Problemas de integridad de los datos
- Problemas con las pruebas:
  - Faltan pruebas
  - Pruebas ineficaces
  - Pruebas escamosas
- Fallos de infraestructura:
  - Fallos de hardware (servidores, dispositivos de red, almacenamiento)
  - Problemas de escalado

    - Fallos de dependencia (servicios de terceros APIs)
    - Problemas de conectividad de red
- Problemas operativos:
    - Errores humanos (mala configuración, cambios accidentales)
    - Supervisar y alertar de los fallos
    - Problemas de planificación de la capacidad
    - Fallos de Backup y restauración
- Incidentes de seguridad:
    - Intentos de acceso no autorizados
    - Violaciones de datos
    - Ataques de denegación de servicio (DoS)
- Interrupciones del servicio de terceros:
    - Interrupciones de los proveedores de servicios en
    - Fallos de DNS
    - Interrupciones en la API externa y en el servicio
- Factores ambientales:
    - Desastres naturales (terremotos, incendios, inundaciones, cortes de energía)
    - Problemas relacionados con el clima

Se trata de un ejemplo no concluyente de un marco de clasificación que puede personalizar para adaptarlo a sus necesidades y a su organización específicas. Recomendamos revisar y actualizar el marco de clasificación periódicamente a medida que el sistema evolucione o surjan nuevos tipos de incidentes.

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

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

A

ABAC

Consulte control de acceso basado en atributos.

servicios abstractos

Consulte servicios gestionados.

ACID

Consulte atomicidad, consistencia, aislamiento y durabilidad.

migración activa-activa

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

migración activa-pasiva

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

función agregada

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

IA

Véase inteligencia artificial.

AIOps

Consulte las operaciones de inteligencia artificial.

anonimización

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

antipatrones

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

control de aplicaciones

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

cartera de aplicaciones

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

inteligencia artificial (IA)

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

operaciones de inteligencia artificial (AIOps)

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

cifrado asimétrico

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

atomicidad, consistencia, aislamiento, durabilidad (ACID)

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

control de acceso basado en atributos (ABAC)

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

origen de datos fidedigno

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

Zona de disponibilidad

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

AWS Marco de adopción de la nube (AWS CAF)

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

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

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

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

B

Un bot malo

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

BCP

Consulte la planificación de la continuidad del negocio.

gráfico de comportamiento

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

sistema big-endian

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

clasificación binaria

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

filtro de floración

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

implementación azul/verde

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

bot

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

botnet

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

branch

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

acceso con cristales rotos

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

estrategia de implementación sobre infraestructura existente

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

caché de búfer

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

capacidad empresarial

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

planificación de la continuidad del negocio (BCP)

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

C

CAF

Consulte el marco AWS de adopción de la nube.

despliegue canario

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

CCoE

Consulte Cloud Center of Excellence.

CDC

Consulte la captura de datos de cambios.

captura de datos de cambio (CDC)

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

ingeniería del caos

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

CI/CD

Consulte la integración continua y la entrega continua.

clasificación

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

cifrado del cliente

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

Centro de excelencia en la nube (CCoE)

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

computación en la nube

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

modelo operativo en la nube

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

etapas de adopción de la nube

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

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

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

CMDB

Consulte la base de datos de administración de la configuración.

repositorio de código

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

caché en frío

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

datos fríos

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

visión artificial (CV)

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

desviación de configuración

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

base de datos de administración de configuración (CMDB)

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

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

paquete de conformidad

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

integración y entrega continuas (CI/CD)

El proceso de automatización de las etapas de origen, compilación, prueba, puesta en escena y producción del proceso de publicación del software. CI/CD is commonly described as a pipeline. CI/CDpuede ayudarlo a automatizar los procesos, mejorar la productividad, mejorar la calidad del código y entregar con mayor rapidez. Para obtener más información, consulte Beneficios de la entrega continua. CD también puede significar implementación continua. Para obtener más información, consulte Entrega continua frente a implementación continua.

CV

Vea la visión artificial.

D

datos en reposo

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

clasificación de datos

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

desviación de datos

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

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

datos en tránsito

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

malla de datos

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

minimización de datos

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

perímetro de datos

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

preprocesamiento de datos

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

procedencia de los datos

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

titular de los datos

Persona cuyos datos se recopilan y procesan.

almacenamiento de datos

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

lenguaje de definición de datos (DDL)

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

lenguaje de manipulación de datos (DML)

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

DDL

Consulte el lenguaje de definición de bases de datos.

conjunto profundo

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

aprendizaje profundo

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

defense-in-depth

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

administrador delegado

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

Implementación

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

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

entorno de desarrollo

Consulte entorno.

control de detección

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

asignación de flujos de valor para el desarrollo (DVSM)

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

gemelo digital

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

tabla de dimensiones

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

desastre

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

recuperación de desastres (DR)

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

DML

Consulte el lenguaje de manipulación de bases de datos.

diseño basado en el dominio

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

DR

Consulte recuperación ante desastres.

detección de deriva

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

DVSM

Consulte el mapeo del flujo de valor del desarrollo.

E

EDA

Consulte el análisis exploratorio de datos.

EDI

Véase intercambio electrónico de datos.

computación en la periferia

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

intercambio electrónico de datos (EDI)

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

cifrado

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

clave de cifrado

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

endianidad

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

punto de conexión

Consulte el punto final del servicio.

servicio de punto de conexión

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

planificación de recursos empresariales (ERP)

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

cifrado de sobre

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

entorno

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

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

epopeya

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

ERP

Consulte planificación de recursos empresariales.

análisis de datos de tipo exploratorio (EDA)

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

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

F

tabla de datos

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

fallan rápidamente

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

límite de aislamiento de fallas

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

rama de característica

Consulte la sucursal.

características

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

importancia de las características

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

transformación de funciones

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

indicaciones de unos pocos pasos

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

FGAC

Consulte el control de acceso detallado.

control de acceso preciso (FGAC)

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

migración relámpago

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

FM

Consulte el modelo básico.

modelo de base (FM)

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

G

IA generativa

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

bloqueo geográfico

Consulta las restricciones geográficas.

restricciones geográficas (bloqueo geográfico)

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

Flujo de trabajo de Gitflow

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

imagen dorada

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

estrategia de implementación desde cero

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

barrera de protección

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

H

HA

Consulte la alta disponibilidad.

migración heterogénea de bases de datos

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

alta disponibilidad (HA)

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

modernización histórica

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

datos retenidos

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

migración homogénea de bases de datos

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

datos recientes

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

hotfix

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

periodo de hiperatención

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

I

IaC

Vea la infraestructura como código.

políticas basadas en identidad

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

aplicación inactiva

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

IIoT

Consulte Internet de las cosas industrial.

infraestructura inmutable

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

VPC entrante (de entrada)

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

migración gradual

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

Industria 4.0

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

infraestructura

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

infraestructura como código (IaC)

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

Internet de las cosas industrial (T) IIo

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

VPC de inspección

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

Internet de las cosas (IoT)

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

interpretabilidad

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

IoT

Consulte Internet de las cosas.

biblioteca de información de TI (ITIL)

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

administración de servicios de TI (ITSM)

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

ITIL

Consulte la biblioteca de información de TI.

ITSM

Consulte Administración de servicios de TI.

L

control de acceso basado en etiquetas (LBAC)

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

zona de aterrizaje

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

modelo de lenguaje grande (LLM)

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

migración grande

Migración de 300 servidores o más.

LBAC

Consulte control de acceso basado en etiquetas.

privilegio mínimo

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

migrar mediante lift-and-shift

Ver 7 Rs.

sistema little-endian

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

LLM

Véase un modelo de lenguaje amplio.

entornos inferiores

Véase entorno.

M

machine learning (ML)

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

rama principal

Ver sucursal.

malware

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

servicios gestionados

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

sistema de ejecución de fabricación (MES)

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

MAP

Consulte Migration Acceleration Program.

mecanismo

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

cuenta de miembro

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

MES

Consulte el sistema de ejecución de la fabricación.

Transporte telemétrico de Message Queue Queue (MQTT)

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

microservicio

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

arquitectura de microservicios

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

Programa de aceleración de la migración (MAP)

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

migración a escala

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

fábrica de migración

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

metadatos de migración

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

patrón de migración

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

Migration Portfolio Assessment (MPA)

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

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

Evaluación de la preparación para la migración (MRA)

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

estrategia de migración

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

ML

Consulte el aprendizaje automático.

modernización

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

evaluación de la preparación para la modernización

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

aplicaciones monolíticas (monolitos)

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

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

MAPA

Consulte la evaluación de la cartera de migración.

MQTT

Consulte Message Queue Queue Telemetría y Transporte.

clasificación multiclase

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

infraestructura mutable

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

O

OAC

Consulte el control de acceso de origen.

OAI

Consulte la identidad de acceso de origen.

OCM

Consulte gestión del cambio organizacional.

migración fuera de línea

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

OI

Consulte integración de operaciones.

OLA

Véase el acuerdo a nivel operativo.

migración en línea

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

OPC-UA

Consulte Open Process Communications: arquitectura unificada.

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

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

acuerdo de nivel operativo (OLA)

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

revisión de la preparación operativa (ORR)

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

tecnología operativa (OT)

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

integración de operaciones (OI)

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

registro de seguimiento organizativo

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

administración del cambio organizacional (OCM)

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

control de acceso de origen (OAC)

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

identidad de acceso de origen (OAI)

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

ORR

Consulte la revisión de la preparación operativa.

OT

Consulte la tecnología operativa.

VPC saliente (de salida)

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

P

límite de permisos

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

información de identificación personal (PII)

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

PII

Consulte la información de identificación personal.

manual de estrategias

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

PLC

Consulte controlador lógico programable.

PLM

Consulte la gestión del ciclo de vida del producto.

policy

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

persistencia políglota

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

evaluación de cartera

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

predicate

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

pulsar un predicado

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

control preventivo

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

entidad principal

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

privacidad desde el diseño

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

zonas alojadas privadas

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

control proactivo

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

gestión del ciclo de vida del producto (PLM)

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

entorno de producción

Consulte el entorno.

controlador lógico programable (PLC)

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

encadenamiento rápido

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

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

seudonimización

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

publish/subscribe (pub/sub)

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

Q

plan de consulta

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

regresión del plan de consulta

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

R

Matriz RACI

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

RAG

Consulte Retrieval Augmented Generation.

ransomware

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

Matriz RASCI

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

RCAC

Consulte control de acceso por filas y columnas.

réplica de lectura

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

rediseñar

Ver 7 Rs.

objetivo de punto de recuperación (RPO)

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

objetivo de tiempo de recuperación (RTO)

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

refactorizar

Ver 7 Rs.

Región

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

regresión

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

volver a alojar

Consulte 7 Rs.

versión

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

trasladarse

Ver 7 Rs.

redefinir la plataforma

Ver 7 Rs.

recompra

Ver 7 Rs.

resiliencia

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

política basada en recursos

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

matriz responsable, confiable, consultada e informada (RACI)

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

control receptivo

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

retain

Consulte 7 Rs.

jubilarse

Ver 7 Rs.

Generación aumentada de recuperación (RAG)

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

rotación

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

control de acceso por filas y columnas (RCAC)

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

RPO

Consulte el objetivo del punto de recuperación.

RTO

Consulte el objetivo de tiempo de recuperación.

manual de procedimientos

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

S

SAML 2.0

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

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

SCADA

Consulte el control de supervisión y la adquisición de datos.

SCP

Consulte la política de control de servicios.

secreta

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

seguridad desde el diseño

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

control de seguridad

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

refuerzo de la seguridad

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

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

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

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

automatización de la respuesta de seguridad

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

cifrado del servidor

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

política de control de servicio (SCP)

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

punto de enlace de servicio

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

acuerdo de nivel de servicio (SLA)

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

indicador de nivel de servicio (SLI)

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

objetivo de nivel de servicio (SLO)

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

modelo de responsabilidad compartida

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

SIEM

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

punto único de fallo (SPOF)

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

SLA

Consulte el acuerdo de nivel de servicio.

SLI

Consulte el indicador de nivel de servicio.

SLO

Consulte el objetivo de nivel de servicio.

split-and-seed modelo

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

SPOF

Consulte el punto único de falla.

esquema en forma de estrella

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

patrón de higo estrangulador

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

subred

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

supervisión, control y adquisición de datos (SCADA)

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

cifrado simétrico

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

pruebas sintéticas

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

indicador del sistema

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

T

etiquetas

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

variable de destino

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

lista de tareas

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

entorno de prueba

Consulte entorno.

entrenamiento

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

puerta de enlace de tránsito

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

flujo de trabajo basado en enlaces troncales

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

acceso de confianza

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

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

ajuste

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

equipo de dos pizzas

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

U

incertidumbre

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

tareas indiferenciadas

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

entornos superiores

Ver entorno.

V

succión

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

control de versión

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

Emparejamiento de VPC

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

vulnerabilidad

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

W

caché caliente

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

datos templados

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

función de ventana

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

carga de trabajo

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

flujo de trabajo

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

GUSANO

Mira, escribe una vez, lee muchas.

WQF

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

escribe una vez, lee muchas (WORM)

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

Z

ataque de día cero

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

vulnerabilidad de día cero

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

aviso de tiro cero

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

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

aplicación zombi

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

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