



Adopción del estándar Matter para los fabricantes de dispositivos de IoT

AWS Guía prescriptiva



AWS Guía prescriptiva: Adopción del estándar Matter para los fabricantes de dispositivos de IoT

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

Introducción	1
Objetivos	1
Entender la materia	3
Protocolo Matter	3
Descripción general de cómo funciona Matter	4
Ventajas de certificar	5
Ventajas para los consumidores	5
Configuración simplificada y administración unificada	5
Más opciones y flexibilidad en el control por voz	6
Ventajas para los fabricantes de dispositivos	7
Certificación única en todos los ecosistemas	7
Reducción de los costes de desarrollo	7
Atención al cliente simplificada	8
Consideraciones sobre la certificación	9
Protocolos de conectividad no IP	9
Limitaciones de hardware	10
Ecosistemas de clientes	10
Los tipos de dispositivos aún no están definidos	11
Una alternativa: utilizar proxy en las puertas de enlace	11
Conectividad a la nube con Matter	13
Habilitar capacidades avanzadas de los dispositivos con conectividad a la nube para terminales de Matter	13
Casos de uso que requieren conectividad a la nube	13
Arquitecturas para habilitar la conectividad a la nube	15
Bridging Matter y las plataformas en la nube de los fabricantes	15
Seguridad	17
Autenticación de	17
Comunicación cifrada	17
No hay actualizaciones ver-the-air	18
Desarrollo con materia	19
¿Usando Alexa	19
Autoridad de certificación privada de AWS soporte para Matter	19
Preguntas frecuentes	21
¿Cuáles son los niveles de membresía de Matter?	21

¿Cómo se benefician de Matter los consumidores de hogares inteligentes? 22

¿Cómo se benefician los fabricantes de dispositivos de Matter? 22

¿Matter reemplaza a Wi-Fi, Bluetooth o Thread? 23

¿Qué es un identificador de proveedor y un identificador de producto? 23

¿Qué dispositivos deben tener la certificación Matter? 24

Mi tipo de producto no está definido actualmente en Matter. ¿Para qué tareas adicionales debo presupuestar tiempo para obtener la certificación Matter de los productos? 24

Algunos de mis dispositivos se conectan directamente a la red Wi-Fi doméstica. ¿Estos dispositivos deben tener la certificación Matter? 24

Recursos 26

 AWS recursos 26

 Alianza de estándares de conectividad (CSA) para IoT 26

Historial de documentos 27

Glosario 28

 # 28

 A 29

 B 32

 C 34

 D 37

 E 42

 F 44

 G 46

 H 47

 I 49

 L 51

 M 52

 O 57

 P 60

 Q 63

 R 63

 S 66

 T 70

 U 72

 V 72

 W 73

 Z 74

..... lxxv

Adopción del estándar Matter para los fabricantes de dispositivos de IoT

Tushar Patel, Vijay Ujjain y David Walters, Amazon Web Services (AWS)

[Febrero de 2024 \(historia del documento\)](#)

Según [Statista](#), se espera que el número de hogares inteligentes en todo el mundo alcance los 780 millones en 2028. Este rápido crecimiento ha traído consigo desafíos en términos de operaciones y administración. Desde el punto de vista del consumidor, cada proveedor de dispositivos tiene un método diferente para integrar el dispositivo doméstico inteligente en una red doméstica a través de una aplicación específica para ese proveedor de dispositivos. Esto dificulta la gestión de una gama cada vez mayor de diversos tipos de dispositivos de distintos proveedores. Del mismo modo, desde el punto de vista de un fabricante de dispositivos, certificar sus productos para hogares inteligentes en distintos ecosistemas aumenta el coste y la complejidad de sus procesos empresariales. Por ejemplo, esto puede requerir diferentes SKU para el mismo modelo de dispositivo. Mantener una aplicación que ofrezca una experiencia de usuario atractiva y ofrecer actualizaciones periódicas supone una sobrecarga adicional, lo que desvía los recursos destinados a centrarse en crear y ofrecer un producto mejor. Tanto los consumidores como los fabricantes de dispositivos se beneficiarían de un estándar común de interoperabilidad para hogares inteligentes. Este estándar permite que los dispositivos de varios proveedores interactúen entre sí de manera fluida, segura y confiable.

El nuevo estándar [Matter](#) presenta una gran oportunidad para los fabricantes de dispositivos de Internet de las cosas (IoT) en el ámbito de los hogares inteligentes. Este estándar tiene como objetivo mejorar la compatibilidad e interoperabilidad entre dispositivos de diferentes fabricantes. Matter es un protocolo de conectividad abierto para hogares inteligentes que permite la comunicación entre dispositivos de IoT, aplicaciones móviles y servicios en la nube.

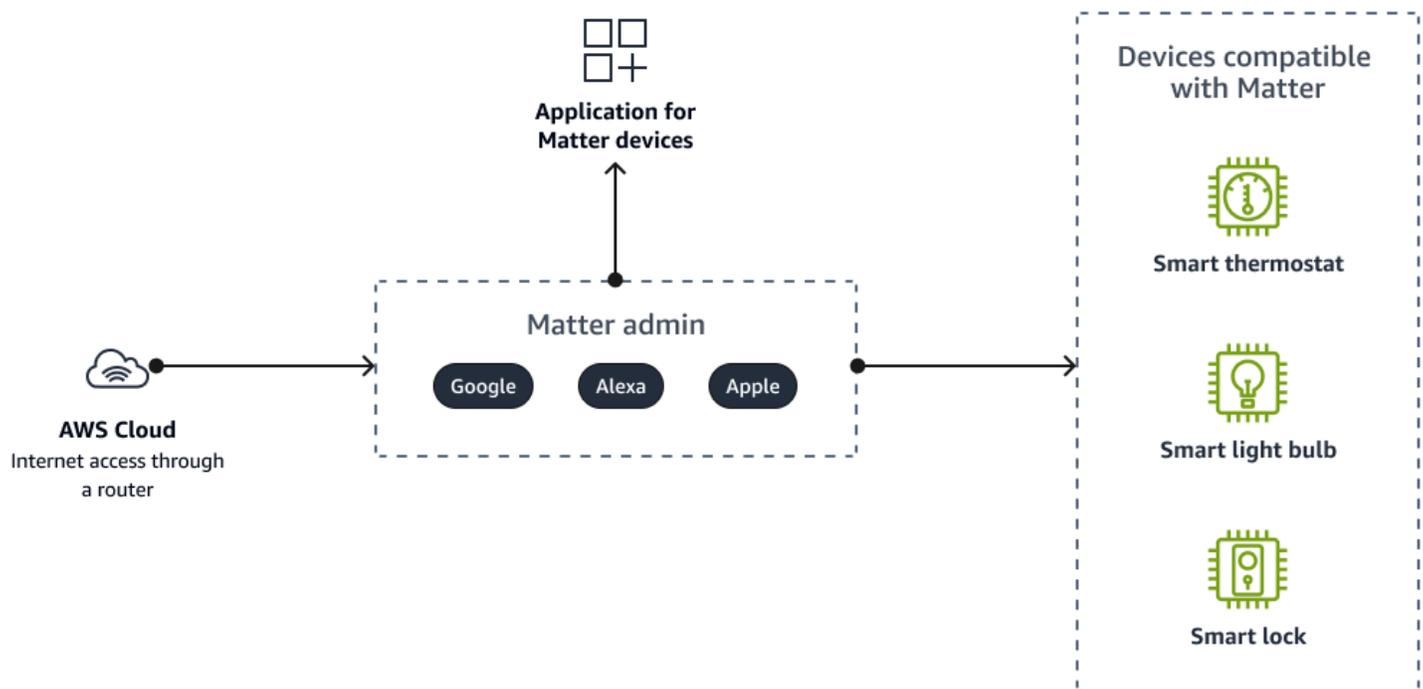
Objetivos

Al integrar el estándar Matter en sus productos, los fabricantes de dispositivos de IoT deben abordar varios desafíos antes de comenzar el desarrollo. Matter ofrece muchas ventajas sobre los protocolos de IoT patentados, como la interoperabilidad, la seguridad, la simplicidad, la confiabilidad y la protección futura de los dispositivos. Sin embargo, la integración de Matter en las implementaciones de IoT nuevas y existentes requiere una planificación y una estrategia cuidadosas. Los fabricantes

quieren orientación sobre el proceso de cumplimiento de Matter para aprovechar los beneficios y evitar dificultades. Esta guía proporciona a los fabricantes de dispositivos de IoT una guía completa sobre la adopción de Matter. Incluye una hoja de ruta clara, desde la estrategia hasta la implementación. Esta guía facilita la transición a Matter y le ayuda a crear productos seguros, interoperables y preparados para el futuro que prosperen en el ecosistema de hogares inteligentes. Con el enfoque estratégico correcto, las organizaciones pueden superar los obstáculos de la adopción de Matter y desarrollar dispositivos IoT innovadores que adopten estándares abiertos.

Esta guía proporciona a los fabricantes de dispositivos una visión general completa de Matter y los pasos necesarios para cumplir con Matter. Describe las ventajas y desventajas de planificar una estrategia de adopción de Matter. La guía también sugiere las mejores prácticas para aprovechar Matter y, al mismo tiempo, seguir respaldando los protocolos inalámbricos existentes, de forma gradual. Para los fabricantes de dispositivos de IoT que buscan soluciones para hogares inteligentes, esta guía puede informar su estrategia de conectividad.

Comprensión del estándar Matter



Protocolo Matter

Matter es un protocolo de conectividad abierto para hogares inteligentes que permite la comunicación entre dispositivos, aplicaciones móviles y servicios en la nube. Desarrollado por la Alianza de Estándares de Conectividad (CSA), Matter simplifica la conectividad y la interoperabilidad para consumidores y fabricantes. Matter es compatible con una amplia gama de categorías de hogares inteligentes. Para los consumidores, Matter ofrece integración, administración unificada y control en todos los ecosistemas. Para los fabricantes, Matter reduce los costos de desarrollo y soporte mediante una certificación única y mediante el desarrollo de aplicaciones. Muchas grandes empresas, como Amazon, Apple y Google, están promoviendo la adopción de Matter. La CSA ofrece cuatro [niveles de membresía](#) según la participación de la organización: promotores, participantes, adoptantes y asociados. Con un fuerte apoyo de la industria, Matter tiene como objetivo proporcionar una conectividad perfecta entre las marcas para los consumidores y agilizar el desarrollo para los fabricantes.

Descripción general de cómo funciona Matter

Matter es un protocolo de nivel de aplicación basado en IP para dispositivos domésticos inteligentes en todos los ecosistemas de proveedores. Funciona en dispositivos que utilizan IPv6. Conceptualmente, Matter se organiza como una colección de nodos de red, que son los puntos finales de Matter. A continuación se presenta un breve resumen de la terminología de la materia:

- Los dispositivos Matter son productos domésticos inteligentes, como bombillas, interruptores, termostatos o cerraduras.
- Un Matter Fabric es la red virtual a la que están conectados todos los dispositivos. Todos los dispositivos comparten la misma raíz de confianza. La estructura forma una topología de red en estrella.
- Un administrador de Matter crea, mantiene y administra la seguridad y los privilegios de todos los dispositivos de la estructura. Un administrador puede ser un hub o una aplicación. Matter tiene una función de administración múltiple, en la que un dispositivo Matter puede formar parte de varias estructuras simultáneamente. Por ejemplo, un único dispositivo Matter puede administrarse tanto por un dispositivo Amazon Alexa como por un dispositivo Google Home, los cuales podrían ser administradores de Matter en la misma red física.
- Un comisario de Matter es un dispositivo que encarga (o incorpora) un nuevo dispositivo Matter a la estructura. Puede ser una aplicación en un teléfono, una pasarela doméstica inteligente o un administrador de Matter.
- Un puente Matter conecta dispositivos sin protocolo IP a una estructura Matter.

Para obtener información sobre las diferentes funciones que el hardware y el software pueden desempeñar en Matter, consulte [Ekeking Under the Hood of Your Matter Smart Home](#) (entrada del blog de la CSA).

Ventajas de certificarse con Matter

La introducción de Matter promete ofrecer ventajas significativas tanto a los consumidores de hogares inteligentes como a los fabricantes que los ofrecen. Al establecer un lenguaje común para los dispositivos inteligentes, Matter pretende desentrañar el fragmentado mercado actual mediante una configuración simplificada, una administración unificada en todas las plataformas y una mayor variedad y flexibilidad en el control por voz.

Para los consumidores, esta experiencia unificada debería hacer que construir y expandir su hogar inteligente sea significativamente menos complejo y abrumador. Los fabricantes de dispositivos también obtienen beneficios significativos al agilizar la certificación, reducir los costos de desarrollo y simplificar la atención al cliente. Ambos grupos se benefician, ya que Matter impulsa una mayor interoperabilidad y reduce las barreras a la adopción de los hogares inteligentes. En general, la certificación según el estándar Matter está destinada a acelerar el crecimiento del mercado de hogares inteligentes al resolver los problemas que lo han frenado hasta ahora.

Temas

- [Ventajas de la certificación Matter para los consumidores de hogares inteligentes](#)
- [Ventajas de la certificación Matter para los fabricantes de dispositivos](#)

Ventajas de la certificación Matter para los consumidores de hogares inteligentes

La introducción de Matter promete ofrecer importantes beneficios a los consumidores. Matter proporciona un lenguaje común para que los dispositivos domésticos inteligentes funcionen juntos sin problemas en las principales plataformas. Al certificar los dispositivos con Matter, los consumidores pueden esperar una configuración y administración más sencillas de su hogar inteligente, así como una mayor flexibilidad y opciones a la hora de controlar sus dispositivos.

Configuración simplificada y administración unificada

Una de las mayores frustraciones a las que se enfrentan los consumidores son los complejos procesos de configuración e incorporación que se requieren para operar diferentes dispositivos domésticos inteligentes y hacer que funcionen juntos. Es posible que cada dispositivo requiera su propia aplicación patentada y una cuenta independiente. Para solucionar este problema, Matter

habilita plug-and-play la funcionalidad para los dispositivos certificados. Incorporar dispositivos certificados por Matter es tan sencillo como conectar el dispositivo a la red doméstica local y, a continuación, utilizar el administrador de Matter, como la aplicación Alexa, para leer el código QR del dispositivo.

Esta experiencia de configuración unificada a través de una sola aplicación significa que los consumidores ya no necesitan hacer malabares con varias aplicaciones independientes para administrar diferentes marcas de dispositivos. Pueden ver y controlar todas sus luces, cerraduras, sensores y mucho más con certificación Matter desde una única interfaz. Los usuarios de Apple HomeKit, Amazon Alexa y Google Assistant se benefician de poder descubrir y controlar los dispositivos Matter sin tener que descargar aplicaciones de fabricantes independientes. La administración simplificada de los dispositivos domésticos inteligentes a través de un sistema unificado reduce la complejidad para los consumidores y hace que construir y ampliar su configuración sea mucho menos difícil.

Más opciones y flexibilidad en el control por voz

El control por voz se ha convertido en una forma popular para que los consumidores interactúen con sus dispositivos domésticos inteligentes. Sin embargo, hoy en día, la elección del asistente de voz suele dictar qué marcas de dispositivos puede controlar con la voz. Matter cambia esta situación al permitir el control por voz en todos los ecosistemas.

Los consumidores obtienen la flexibilidad de elegir el ecosistema de asistentes de voz que mejor se adapte a sus necesidades, sin tener que preocuparse por la compatibilidad de los dispositivos. Un usuario que se sienta cómodo con el Asistente de Google puede controlar sus dispositivos certificados por Matter con la voz, incluso si los dispositivos se fabricaron originalmente para Alexa o HomeKit para otros mercados.

Esta compatibilidad cruzada del control por voz crea un entorno más abierto que ofrece a los usuarios más opciones. Pueden elegir los dispositivos en función de las características y el precio, en lugar de la compatibilidad con un único ecosistema. Si un usuario quiere cambiar de asistente de voz en el futuro, la configuración de su hogar inteligente actual puede adaptarse fácilmente a ellos, ya que todos los dispositivos hablan el lenguaje común Matter.

Ventajas de la certificación Matter para los fabricantes de dispositivos

Además de ayudar a los consumidores, la certificación Matter también ofrece beneficios significativos a los fabricantes de dispositivos inteligentes. Al adoptar el estándar Matter, las organizaciones pueden obtener ventajas que reducen los costos y amplían el alcance de sus clientes.

Certificación única en todos los ecosistemas

En la actualidad, para garantizar la compatibilidad entre ecosistemas como Alexa HomeKit y Google Home, los fabricantes deben pasar por varios procesos de certificación largos y costosos con cada organización. Matter cambia esta situación al establecer una única certificación común.

Los fabricantes de dispositivos solo necesitan certificar sus productos una vez según el estándar Matter para que sean compatibles con los principales ecosistemas de hogares inteligentes y los asistentes de voz. Esto agiliza el desarrollo y reduce los costes de certificación de forma significativa en comparación con la situación actual. Ya no es necesario gastar recursos en mantener certificaciones independientes a medida que se actualizan los productos. Una sola certificación Matter también prepara los productos para el futuro y garantiza la compatibilidad incluso cuando surgen nuevos ecosistemas.

Reducción de los costes de desarrollo

Matter también ayuda a reducir los costes de desarrollo para los fabricantes. Al adoptar un estándar común de conectividad y seguridad, las organizaciones se benefician de los componentes de infraestructura compartidos que contribuyen al proyecto general de Matter.

Por ejemplo, los fabricantes ya no necesitan incluir sus propios enrutadores Thread Border patentados en sus productos, lo que transfiere esta responsabilidad a los fabricantes de concentradores. Los controladores y bibliotecas de código abierto compartidos reducen aún más el trabajo de ingeniería redundante. Los mecanismos comunes de descubrimiento de servicios y configuración de dispositivos hacen que sea necesario desarrollar menos aplicaciones a medida. Estas reducciones en los costos de infraestructura y desarrollo de aplicaciones pueden repercutir en los consumidores en forma de dispositivos domésticos inteligentes más asequibles.

Atención al cliente simplificada

La fragmentación actual del mercado de los hogares inteligentes genera una gran carga de atención al cliente para los fabricantes. Los consumidores suelen tener problemas de conectividad, configuración y compatibilidad que requieren una solución de problemas. Matter tiene como objetivo reducir estos problemas mediante la estandarización de las funciones principales.

Cuando se producen problemas, los protocolos subyacentes comunes de Matter permiten a las empresas diagnosticar y resolver los problemas de conectividad más fácilmente sin tener que considerar múltiples ecosistemas. Esto agiliza el proceso de soporte. Con una sola aplicación y una compatibilidad de voz común, a los clientes también les resulta más fácil aprender a usar los dispositivos, lo que reduce la necesidad de asistencia en muchos casos. La simplificación de la experiencia del cliente y la solución de problemas que ofrece Matter ayudan a reducir los costes de soporte a largo plazo para los fabricantes.

Consideraciones para la estrategia de certificación Matter

Matter permite la interoperabilidad entre diferentes plataformas y dispositivos domésticos inteligentes. Sin embargo, la certificación con Matter puede no ser siempre la mejor opción para los fabricantes de dispositivos. Los costos de implementación y certificación pueden no tener sentido práctico o financiero, según el tipo de dispositivo y los casos de uso. En esta sección se analizan algunos de los principales motivos por los que un fabricante podría optar por no certificar determinados dispositivos con Matter.

Si bien el objetivo del estándar Matter es simplificar el desarrollo y permitir la compatibilidad universal, algunos tipos de dispositivos domésticos inteligentes pueden enfrentarse a obstáculos prácticos para obtener la certificación que superan los beneficios. En el caso de los productos con restricciones estrictas, protocolos no relacionados con IP, audiencias limitadas o tipos de dispositivos no definidos en Matter, obtener la certificación Matter podría no ser la mejor estrategia inicialmente. Estas podrían ser las razones por las que un fabricante podría evitar adoptar Matter. Sin embargo, Matter sí permite que los dispositivos de puerta de enlace habilitados para IP actúen como proxy para puntos finales que no son IP. Para algunos dispositivos heredados, un enfoque de puerta de enlace puede ser una forma viable de lograr la compatibilidad con Matter y, al mismo tiempo, evitar un rediseño completo del dispositivo.

A medida que el estándar Matter evolucione y su alcance se amplíe para cubrir más casos de uso, los argumentos a favor de la certificación podrían fortalecerse con el tiempo, incluso para estas categorías de productos. Los fabricantes de dispositivos deben evaluar sus situaciones y hojas de ruta específicas para determinar el mejor enfoque en relación con el cumplimiento de la normativa Matter. En muchas situaciones, pueden existir razones técnicas o comerciales sólidas para optar por no recibir la certificación, al menos temporalmente.

Protocolos de conectividad no IP

Para adoptar el estándar Matter, los dispositivos deben funcionar en redes IP, como Wi-Fi, Ethernet y Thread. Los protocolos inalámbricos no IP, como Zigbee, Z-Wave y Bluetooth LE, se utilizan habitualmente en dispositivos con poco ancho de banda. Estos protocolos requieren un traductor de protocolos adicional que no esté basado en IP a IP para que sean compatibles con Matter. La actualización del módulo de comunicación o la introducción de una pasarela de traducción generalmente aumenta el costo de hardware del dispositivo.

Añadir la compatibilidad con pilas IP implica asignar más memoria y potencia de procesamiento para la gestión de la red. Esto podría superar las capacidades de los dispositivos de bajo coste y consumo de energía extremadamente bajos. La adición de memoria o flash adicionales para admitir la tecnología IP también aumentaría los costos de fabricación y reduciría la duración de la batería. Para los casos de uso en los que lo único que se necesita es encender y apagar la alimentación o los datos de los sensores, los protocolos que no son IP pueden ofrecer una solución eficaz.

Básicamente, Matter descarta certificar cualquier dispositivo que se base en estándares inalámbricos patentados que no sean IP. Esto podría limitar a los fabricantes que desean utilizar métodos de conectividad alternativos para sus productos de gama baja. Si bien los protocolos basados en IP, como Wi-Fi y Ethernet, son necesarios para interactuar con diferentes ecosistemas, los estándares no IP siguen siendo válidos para la conectividad básica de sensores y conmutadores en algunas aplicaciones.

Limitaciones de hardware

Otro desafío es que Matter requiere un nivel mínimo de potencia de procesamiento y memoria en el dispositivo para admitir la pila de software necesaria. Sin embargo, los dispositivos domésticos inteligentes más básicos suelen tener capacidades de chip integradas muy limitadas, debido a las limitaciones de costo y tamaño.

Por ejemplo, un sensor simple de puerta o ventana puede contener solo un microcontrolador con menos de 100 KB de memoria flash y 10 KB de RAM. Esto no proporciona suficiente espacio de almacenamiento y procesamiento para una implementación completa de Matter. Añadir silicio más potente y caro aumentaría considerablemente la lista de materiales.

En los casos en que el coste y el tamaño son las principales prioridades, es posible que los fabricantes descubran que los requisitos de Matter no se ajustan a sus presupuestos de hardware. La certificación de sensores, conmutadores o controladores muy básicos con Matter podría forzar actualizaciones de hardware innecesarias que afectarían a la asequibilidad.

Ecosistemas de clientes

Otro factor a tener en cuenta es si la base de clientes objetivo de un fabricante utiliza plataformas para hogares inteligentes que sean compatibles con Matter. Si la mayoría de los consumidores de ese segmento no utilizan los controladores Matter ni los concentradores y aplicaciones compatibles con Matter, es posible que haya pocos incentivos para certificar los productos.

Por ejemplo, una empresa que se centre en atender las necesidades de los usuarios de edad avanzada podría darse cuenta de que sus clientes tienen configuraciones sencillas sin administradores de Matter. O bien, los entusiastas de la automatización del hogar do-it-yourself (hágalo usted mismo) pueden preferir soluciones personalizadas y no necesitar la plug-and-play experiencia de Matter en todas las marcas.

En situaciones en las que el grupo demográfico objetivo no utiliza la infraestructura de Matter, la certificación añade complejidad sin beneficios claros. Sería mejor invertir los recursos en optimizar la experiencia del usuario en las plataformas pertinentes en lugar de desviar los esfuerzos hacia el cumplimiento de Matter.

Los tipos de dispositivos aún no están definidos

Actualmente, Matter solo define los perfiles y las especificaciones de los dispositivos para las categorías más comunes de hogares inteligentes, como la iluminación, la climatización, las cerraduras, las persianas y el entretenimiento. Cualquier tipo de producto especializado fuera de estas áreas definidas debe usar un perfil personalizado hasta que el tipo de dispositivo esté estandarizado. Las categorías de dispositivos que no figuran en las listas verticales, como los controladores de riego, los equipos para piscinas y los electrodomésticos especializados, aún no pueden usar Matter.

Si una empresa desarrolla tipos de dispositivos únicos que no están incluidos en los perfiles de Matter existentes, la certificación no será posible hasta que se redacten nuevos perfiles. Esto podría retrasar el lanzamiento de un nuevo producto y esperar a que Matter amplíe su alcance.

En lugar de postergar el lanzamiento de innovaciones, es posible que algunos fabricantes prefieran lanzar soluciones de nicho al mercado antes por medios patentados. Certificar más tarde sigue siendo una opción una vez que los perfiles relevantes hayan madurado. Para aprovechar las ventajas de ser el primero en actuar, en algunos casos puede ser preferible direct-to-consumer prescindir de Matter.

Una alternativa: utilizar proxy en las puertas de enlace

En situaciones en las que un dispositivo terminal tiene limitaciones que impiden la certificación Matter directa, un enfoque alternativo consiste en utilizar la capacidad Matter del dispositivo a través de una pasarela. La puerta de enlace sirve de puente que se traduce entre el protocolo inalámbrico local del terminal y el protocolo Matter basado en IP.

Por ejemplo, un sensor de temperatura básico que se comunica a través de un estándar de radio patentado podría seguir apareciendo como un dispositivo Matter para el administrador de Matter. La puerta de enlace recibe los datos de los sensores en una interfaz que no es IP, pero expone a los controladores entidades Matter virtuales que representan esos datos a través de IP. Esto le permite utilizar el hardware existente y obtener algunos beneficios de interoperabilidad a través de la puerta de enlace.

Por supuesto, esto añade complejidad a los desarrolladores y requiere que las puertas de enlace admitan la capa de traducción necesaria. Sin embargo, podría ser un compromiso viable en los casos en que la certificación directa sea demasiado difícil para el propio dispositivo. Los proxies podrían ayudar a las soluciones de bajo consumo o especializadas a participar en los ecosistemas de Matter sin una revisión completa del hardware.

Conectividad a la nube con Matter

Si bien Matter permite la interoperabilidad básica de los dispositivos locales, se requiere una conectividad adicional a la nube para ofrecer over-the-air actualizaciones sólidas, datos de telemetría, administración remota e integración con los servicios patentados de los proveedores. Los fabricantes de dispositivos tienen opciones, como enviar un hub Matter Gateway, utilizar un hub doméstico certificado por Matter o integrar la conectividad directa a la nube en los terminales. Están surgiendo estándares para la matter-to-cloud conectividad M, pero los fabricantes aún necesitan integrar paquetes de software de conectividad adicionales en los dispositivos Matter. Para ofrecer todo el valor de los dispositivos domésticos inteligentes en áreas como el diagnóstico y las nuevas actualizaciones de funciones, los fabricantes de Matter deben considerar la integración en la nube, más allá de la operación local básica.

Habilitar capacidades avanzadas de los dispositivos con conectividad a la nube para terminales de Matter

El estándar Matter promete unificar los dispositivos de IoT de diferentes proveedores a través de un protocolo común. Especifica cómo los dispositivos domésticos inteligentes se descubren, se comunican e interoperan entre sí en la red local mediante tecnologías de red basadas en IP, como Ethernet, Wi-Fi y Thread. Esta interoperabilidad local permite que los dispositivos certificados por Matter de diferentes proveedores trabajen juntos sin problemas para actividades como la automatización de escenas y el control por voz. Sin embargo, Matter no define las interfaces en la nube ni requiere conectividad a Internet para los terminales del dispositivo.

Hoy en día, muchos dispositivos inteligentes dependen de una conectividad adicional a la nube para funciones clave, como las actualizaciones over-the-air (OTA), el acceso remoto y las integraciones con las plataformas de los fabricantes. Los fabricantes de dispositivos que desean crear productos compatibles con Matter y, al mismo tiempo, conservar una funcionalidad avanzada se enfrentan a algunas consideraciones de diseño a la hora de complementar Matter con conectividad a la nube. Si bien la integración básica del control local y el asistente de voz funcionan para dispositivos Matter simples, se requiere una conectividad adicional a la nube para habilitar capacidades más avanzadas.

Casos de uso que requieren conectividad a la nube

Si bien Matter gestiona la interoperabilidad de los dispositivos locales, la conectividad adicional a la nube permite varias funciones importantes de los dispositivos domésticos inteligentes:

- **Actualizaciones O ver-the-air (OTA):** la entrega de actualizaciones de firmware y software a través de Internet permite a los proveedores mejorar fácilmente los dispositivos que ya están desplegados. Sin la OTA, las actualizaciones se gestionarían manualmente. Si bien el estándar Matter describe cómo se gestionan y envían las actualizaciones OTA a los puntos finales certificados por Matter, depende de la funcionalidad compatible con el hub Matter al que esté conectado el punto final. Además, existen restricciones en cuanto a las actualizaciones que se proporcionan al punto final. Por ejemplo, cuando el punto final solicita una actualización, solo se proporciona la última actualización disponible. Todos los dispositivos del mismo tipo reciben esa única actualización. No existe la opción de realizar una actualización secuencial o incluso anular o eliminar una actualización por parte de la OTA. Habilitar la conectividad a la nube en el terminal puede mitigar esta falta de una gestión pormenorizada de las actualizaciones de las OTA.
- **Acceso y control remotos:** para acceder a los dispositivos y controlarlos de forma remota desde fuera de la red doméstica se necesita un punto final en la nube. Matter, tal como se define actualmente, solo admite el acceso local. Si bien un terminal Matter se puede controlar con una aplicación de usuario dentro de la red local, el control remoto solo está disponible si es compatible con el hub Matter. Aun así, por lo general, solo están disponibles los controles remotos básicos.
- **Telemetría y diagnóstico:** la agregación de datos de campo, como registros de errores y flujos de sensores, en la nube permite a los proveedores monitorear el estado de los dispositivos e identificar problemas. Si bien Matter admite los diagnósticos relacionados con la radio y los protocolos a través del clúster de diagnóstico general, cualquier diagnóstico detallado específico del dispositivo requiere conectividad a la nube para que el fabricante pueda recuperar los datos del dispositivo.
- **Integraciones específicas del proveedor:** todas las funciones y tipos de datos personalizados que no estén definidos en la especificación Matter requieren conectividad con las plataformas en la nube de los proveedores.
- **Integraciones externas:** la conexión a servicios de terceros, como asistentes de voz que no estén en el ecosistema Matter o pasarelas de pago de terceros (según sea necesario en cada caso de uso), requiere conectividad a Internet ajena al administrador de Matter.

Dado que estas capacidades fundamentales dependen de la conectividad a la nube, los terminales de Matter suelen necesitar opciones adicionales para acceder a Internet.

Arquitecturas para habilitar la conectividad a la nube

En el caso de los dispositivos Matter, existen tres enfoques generales para proporcionar la conectividad a la nube necesaria y, al mismo tiempo, cumplir con las especificaciones de operación locales.

Concentrador doméstico inteligente con puerta de enlace integrada

Algunos fabricantes de dispositivos pueden optar por ofrecer un hub doméstico patentado que incorpore tanto el administrador Matter como una puerta de enlace a sus servicios en la nube. Este hub doméstico gestionaría los terminales Matter conectados de forma local según el estándar y, al mismo tiempo, facilitaría las conexiones a la nube para funciones avanzadas. El hub podría admitir las actualizaciones de OTA, el acceso remoto y la recopilación de telemetría para los puntos finales.

Transfiera la conectividad en la nube a un centro Matter existente

En lugar de incluir un hub personalizado, los dispositivos podrían diseñarse para conectarse con hubs Matter como Amazon Echo o Google Home para conectarse a Internet. En este caso, el hub Matter existente gestiona la comunicación de los dispositivos locales de acuerdo con el estándar y también proporciona una puerta de enlace a la nube para los puntos finales que lo requieran. Esto aprovecha la infraestructura que quizás ya tengan los consumidores. Sin embargo, este enfoque depende del nivel de soporte que ofrezca el Matter Hub para las funciones que no estén especificadas como normativas para los concentradores Matter en el estándar.

Conectividad directa a la nube en los puntos finales

Los dispositivos con conectividad directa a Internet, como el Wi-Fi, podrían integrar una conectividad independiente para la red local Matter y para los servicios en la nube de los proveedores. Esto permite que el dispositivo actúe como su propia puerta de entrada a la nube. Sin embargo, se necesitan soluciones para los puntos finales no Wi-Fi que se basan en protocolos como Thread. Esto permite que los dispositivos se conecten a la nube de forma independiente, pero puede que no sea posible en el caso de dispositivos simples, de bajo costo y que funcionan con baterías.

Bridging Matter y las plataformas en la nube de los fabricantes

Si bien Matter simplifica la interoperabilidad local, se requieren esfuerzos adicionales para conectar sin problemas los sistemas de administración de Matter y las plataformas en la nube de los fabricantes. Organizaciones como Connectivity Standards Alliance (CSA) están trabajando para

estandarizar la forma en que los dispositivos Matter interactúan con la nube para funciones como las actualizaciones de OTA. La adopción generalizada de estándares para esta conectividad a la nube facilitaría el desarrollo a los fabricantes de dispositivos.

La ruta óptima depende de los casos de uso, los precios y los modelos de negocio de productos específicos. Está claro que se necesita un acceso sólido a los servicios en la nube para aprovechar todas las funciones que esperan los consumidores de hogares inteligentes, incluso en el caso de los dispositivos compatibles con Matter que se centran en la interoperabilidad local. Los fabricantes de dispositivos tienen la oportunidad de utilizar Matter para lograr la interoperabilidad y, al mismo tiempo, ofrecer las capacidades avanzadas mediante una conectividad en la nube cuidadosamente diseñada.

Seguridad

La seguridad desde el diseño es la práctica de incorporar funciones de seguridad durante la etapa de diseño del dispositivo, y no como una idea de último momento durante las últimas etapas de desarrollo. La comunicación cifrada y las actualizaciones over-the-air (OTA) son ejemplos de seguridad desde el diseño. Matter proporciona una base sólida para los dispositivos domésticos inteligentes al implementar la seguridad desde el diseño, empezando por una planta de fabricación confiable y segura. Los dispositivos Matter solo los pueden fabricar y aprovisionar los propietarios de una autoridad de certificación (CA) conocida y confiable de la Autoridad de Atestación de Productos (PAA).

Autenticación de

Los dispositivos Matter deben autenticarse entre sí y ante un controlador antes de poder comunicarse. Solo los dispositivos autorizados pueden conectarse a la estructura Matter. Durante la fabricación, los dispositivos se aprovisionan con una identidad única y un certificado X.509, que se conoce como certificado de atestación de dispositivos (DAC). Cuando el dispositivo intenta conectarse a Matter Fabric por primera vez, el dispositivo encargado comprueba la validez del DAC y comprueba que está firmado por una entidad certificadora intermedia de certificación de productos (PAI) conocida y de confianza. El dispositivo encargado también comprueba si el dispositivo que intenta conectarse a la red cumple con las especificaciones, los protocolos y los estándares de seguridad de Matter. El dispositivo solo tiene acceso a la estructura Matter si todas las comprobaciones se realizan correctamente.

Comunicación cifrada

Una vez que el dispositivo tiene acceso a Matter Fabric, todos los datos que se transmiten entre los dispositivos se protegen mediante un cifrado seguro. La integridad de los datos se preserva mediante un enfoque de varios niveles. El comisario de asuntos realiza el intercambio de claves y la verificación de firmas mediante la curva ECC-256 secp256r1. Una vez intercambiadas las claves, los dispositivos Matter cifran los datos en tránsito mediante el AES-256. Para cada mensaje, los dispositivos utilizan el algoritmo SHA-256 para verificar que los datos no se hayan manipulado durante la transmisión.

No hay actualizaciones ver-the-air

El estándar Matter también exige que los dispositivos implementen una sólida postura de seguridad para las actualizaciones over-the-air (OTA). La OTA es una parte fundamental del ecosistema de hogares inteligentes, ya que los dispositivos pueden recibir actualizaciones de seguridad junto con nuevas funciones. Cada actualización del firmware de los dispositivos Matter debe estar firmada por una clave privada del fabricante. El dispositivo verifica la firma de la carga útil mediante la clave pública asimétrica correspondiente. Una vez verificada la firma de la carga útil, el dispositivo puede enviar la imagen a su gestor de arranque y restablecerla. Durante el proceso de arranque, el dispositivo debe volver a comprobar la imagen para asegurarse de que no ha sido manipulada y también comprobar que está ejecutando la última versión conocida.

Desarrollo con materia

¿Usando Alexa

Amazon ofrece un conjunto completo de herramientas para el desarrollo de Matter. Estas herramientas proporcionan un camino rápido para crear productos Matter que sean compatibles con los principales ecosistemas y que funcionen a la perfección con Amazon Alexa.

Programa: funciona con Alexa

Este programa garantiza que sus dispositivos conectados a Alexa brinden una excelente experiencia al cliente. El distintivo Works with Alexa (WWA) aumenta la confianza de los clientes, lo que contribuye a fomentar la preferencia por los dispositivos certificados. Para obtener más información, consulte [Anuncio del lanzamiento de Matter y Presentación de Works with Alexa \(WWA\) para dispositivos Matter](#) (entrada del blog de Amazon).

SDK: desarrolle Matter con Alexa

Este SDK le permite añadir conectividad Matter local a su dispositivo y, al mismo tiempo, incluye conectividad gestionada en la nube, inteligencia empresarial y compatibilidad con OTA. Para [obtener más información, consulta Saca el máximo partido a Matter con Alexa](#).

Kit: kit para desarrolladores Alexa Ambient Home

Este kit te ayuda a integrarte con dispositivos de todos los protocolos para construir un hogar inteligente unificado y ambiental con Alexa. Para obtener más información, consulta [Amazon Alexa](#).

Punto final: punto final comisionable

En el caso de los dispositivos Matter conectados con habilidades, la API Commissionable Endpoint crea una conexión local basada en Matter con los dispositivos Alexa sin necesidad de que el cliente tenga que realizar ninguna acción con su permiso. Para obtener más información, consulte [Alexa.Commissionable](#) Interface 1.0 (Alexa Skills Kit).

Autoridad de certificación privada de AWS soporte para Matter

AWS Private Certificate Authority (Autoridad de certificación privada de AWS) proporciona orientación sobre el uso del estándar Matter.

DAC para Matter

Matter requiere un certificado de certificación de dispositivos (DAC), que debe ser emitido por una CA de certificación de dispositivos que cumpla con la política de certificación (CP) de Matter de infraestructura de clave pública (PKI). Los proveedores de dispositivos pueden utilizar para hacer lo siguiente: Autoridad de certificación privada de AWS

- Aloje a la autoridad de certificación (CA) de la Autoridad de Atestación de Productos (PAA)
- Organice la CA de certificación de productos intermedia (PAI)
- Emita, firme y mantenga el DAC de cada dispositivo

Para obtener más información, consulte [Uso AWS Private Certificate Authority para emitir certificados de atestación de dispositivos para Matter](#) en el AWS blog de seguridad.

Infraestructura para Matter

AWS proporciona un ejemplo que demuestra el uso de [AWS Cloud Development Kit \(AWS CDK\)](#) para configurar la infraestructura de PKI para Matter. Se utiliza Autoridad de certificación privada de AWS para cumplir los requisitos de la PKI CP de Matter. Para obtener más información, consulte el proyecto [Matter PKI CDK](#) en GitHub

Ejemplos de Java

Autoridad de certificación privada de AWS proporciona ejemplos de Java para crear certificados de la Autoridad de certificación de productos (PAA), certificados intermedios de certificación de productos (PAI) y certificados de atestación de dispositivos (DAC) compatibles con la materia. Para obtener más información, consulte [Uso de la Autoridad de certificación privada de AWS API para implementar el estándar Matter \(ejemplos de Java\) en la documentación](#). AWS Private Certificate Authority

Guía para el cumplimiento de la PKI de Matter

Esta [guía de cumplimiento de Matter PKI](#) explica cómo implementar y demostrar el cumplimiento de los requisitos de CP de la CSA Matter PKI. Proporciona información sobre cómo puede utilizarla para crear y operar autoridades de certificación (Autoridad de certificación privada de AWS CA) que cumplan con las normas de certificación (CA).

Preguntas frecuentes

¿Cuáles son los niveles de membresía de Matter?

A partir de enero de 2023, Matter tiene los siguientes cuatro niveles de membresía.

Tipo de miembro	Cuota anual de membresía (USD)	Descripción
Promotor	105.000 dólares	Dirija la alianza con la aprobación final de todos los estándares, ocupe un puesto en la junta y participe en los comités de la junta
Participante	20 000\$	Contribuya a los estándares y acceda a los borradores de especificaciones para lanzarlos al mercado más rápido
Adoptante	7.000 dólares	Utilice las especificaciones aprobadas para fabricar y certificar productos
Asociado	0 dólares*	Etiquete un producto certificado mediante el programa de transferencia de certificaciones

*Para los miembros asociados que etiquetan un producto con una marca blanca o le cambian la marca, el pago cuesta una cuota inicial de 2.500\$ (USD) por producto y una cuota continua de 500\$ por producto al año.

El nivel de membresía que elijas depende de tu interés en certificar un producto (adoptante) o definir el tipo de producto dentro de la norma (participante). Para obtener más información sobre los niveles de membresía, consulte [Impact the Future of the IoT](#) en el sitio web de la CSA.

¿Cómo se benefician de Matter los consumidores de hogares inteligentes?

Los consumidores se benefician de Matter de las siguientes maneras:

- Integración simplificada de un dispositivo Matter en casa
- Administración unificada de todos los dispositivos domésticos inteligentes a través de una sola aplicación
- Control de dispositivos desde uno o más asistentes de voz de diferentes ecosistemas

Para obtener más información, consulte la sección [Ventajas de la certificación Matter para los consumidores de hogares inteligentes](#) de esta guía.

¿Cómo se benefician los fabricantes de dispositivos de Matter?

Los fabricantes de dispositivos se benefician de Matter de las siguientes maneras:

- Una única certificación para un dispositivo en lugar de varias certificaciones para cada ecosistema, como Amazon Alexa o Google Home.
- El desarrollo de la aplicación ya no es necesario
- Se redujeron los costos de los materiales al no tener que enviar los elementos de infraestructura (como un router Thread Border)
- Reducción de los costes de asistencia a los clientes que tienen problemas de infraestructura y conectividad

Para obtener más información, consulte la sección [Ventajas de la certificación Matter para los fabricantes de dispositivos](#) de esta guía.

¿Matter reemplaza a Wi-Fi, Bluetooth o Thread?

No, Matter es un protocolo de nivel de aplicación que se ejecuta en redes IP. Los dispositivos que utilizan Wi-Fi, Ethernet o Thread para la conectividad pueden obtener la certificación Matter. En la siguiente tabla se resume la diferencia entre Matter y Wi-Fi, Bluetooth y Thread.

Característica	¿Materia	Wifi	Bluetooth	Thread
Finalidad	Comunicación doméstica inteligente	Acceso a Internet y transferencia de datos	Comunicación inalámbrica de corto alcance	Redes en malla inalámbrica de bajo consumo
Range	Varía según el protocolo subyacente	Hasta 300 pies	Hasta 30 pies	Hasta 300 pies
Ancho de banda	Varía según el protocolo subyacente	Hasta 10 gigabits por segundo	Hasta 2 megabits por segundo	Hasta 250 kilobits por segundo
Consumo eléctrico	Varía según el protocolo subyacente	Relativamente alto	Relativamente bajo	Muy bajo
Seguridad	Varía según el protocolo subyacente	WPA2, WPA3	Conexiones seguras AES, BLE	AES
Costo	Varía según el dispositivo	Relativamente económico	Relativamente barato	Relativamente caro

¿Qué es un identificador de proveedor y un identificador de producto?

Los miembros de la CSA pueden solicitar un identificador de proveedor que los identifique como proveedores. De ahora en adelante, a los productos de la empresa se les asigna este identificador

y se puede rastrear hasta su origen. Además, reciben un identificador de producto único. El código numérico de 16 dígitos acompaña a los productos, como un número de pasaporte, y los hace tan inconfundibles como el vendedor.

¿Qué dispositivos deben tener la certificación Matter?

Todos los dispositivos que necesiten autenticarse y formar parte de la estructura Matter deben contar con la certificación Matter. Sin embargo, los dispositivos que estén diseñados para interactuar únicamente con el hub especificado por el proveedor mediante un protocolo no estándar (propietario) no se beneficiarían del proceso de certificación Matter. Por ejemplo, un hub de un sistema de seguridad doméstico inteligente debe estar certificado como compatible con Matter, pero un sensor de puerta o ventana que se comuniquen con el hub no necesita estar certificado como compatible con Matter. La decisión de obtener la certificación Matter de un producto se debe principalmente a esta consideración.

Mi tipo de producto no está definido actualmente en Matter. ¿Para qué tareas adicionales debo presupuestar tiempo para obtener la certificación Matter de los productos?

Las especificaciones de Matter no son compatibles con todos los tipos de dispositivos. Si su tipo de dispositivo no es compatible, el primer paso es unirse a la CSA como participante. Esto requiere una inversión financiera y de tiempo en la CSA. Como miembro participante, usted lidera la definición de los tipos de dispositivos y tiene acceso a los borradores de especificaciones que permiten una go-to-market estrategia más rápida. Para obtener más información sobre los niveles de membresía, consulte [Impact the Future of the IoT](#) en el sitio web de la CSA.

Algunos de mis dispositivos se conectan directamente a la red Wi-Fi doméstica. ¿Estos dispositivos deben tener la certificación Matter?

La certificación Matter puede beneficiar a los dispositivos que se conectan directamente a la red doméstica inteligente, ya que pueden conectarse a la estructura Matter. Esto permite a los consumidores controlar los dispositivos a través de sus asistentes virtuales en la misma estructura Matter. Sin embargo, los consumidores deben usar una aplicación específica para cada dispositivo

para cualquier operación que sea específica del proveedor y no esté definida en la especificación Matter.

Recursos

AWS recursos

- [Aprovecha Matter al máximo con Alexa](#)
- [Anunciamos el lanzamiento de Matter y presentamos Works with Alexa \(WWA\) para dispositivos Matter](#) (blog de Amazon Alexa)

Alianza de estándares de conectividad (CSA) para IoT

- [Sitio web de la CSA](#)
- [Descripción general del proceso de certificación de la CSA](#)
- [Proveedores de pruebas autorizados por la CSA](#)
- [Especificaciones de la materia](#)

Historial del documento

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	—	5 de febrero de 2024

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.

antipatronos

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 CCoE](#) en el blog de estrategia Nube de AWS empresarial.

computación en la nube

La tecnología en la nube que se utiliza normalmente para la administración de dispositivos de IoT y el almacenamiento de datos de forma remota. La computación en la nube suele estar 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 CCoE, establecer un modelo de operaciones)

- Migración: migración de aplicaciones individuales
- Reinención: 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 o Bitbucket Cloud. Cada versión del código se denomina rama. En una estructura de microservicios, cada repositorio se encuentra dedicado a una única funcionalidad. Una sola canalización de CI/CD puede utilizar varios repositorios.

caché en frío

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

datos fríos

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

visión artificial (CV)

Campo de la [IA](#) que utiliza el 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/CD puede 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](#) 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

laC

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.

I

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 (IIoT)

El uso de sensores y dispositivos conectados a Internet en los sectores industriales, como el productivo, el eléctrico, el automotriz, el sanitario, el de las ciencias de la vida y el de la agricultura. Para obtener más información, consulte [Creación de una estrategia de transformación digital 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 dismantelar 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 versión original de inglés, prevalecerá la versión en inglés.