Engineer

AWS

la plataforma de nube de Amazon

Qué es

AWS, abreviatura de Amazon Web Services, es el negocio de Amazon que alquila capacidad informática por hora y por gigabyte: servidores virtuales, almacenamiento de archivos, bases de datos gestionadas, redes privadas, colas y un largo catálogo de otros servicios, todos activados mediante una misma API y facturados a una sola cuenta. Amazon lo vende desde 2006. Dos de sus servicios más conocidos explican buena parte del resto. Amazon EC2 alquila máquinas virtuales, que AWS llama instancias, y Amazon S3 almacena archivos como objetos dentro de contenedores llamados buckets.

En el vocabulario de la definición de NIST, AWS es una nube pública: cualquiera con una tarjeta de pago puede abrir una cuenta, los recursos aparecen en cuestión de minutos y se mide cada segundo o gigabyte de uso. Suele compararse con Azure de Microsoft y Google Cloud, que venden componentes muy similares con otros nombres. Lo que AWS llama una instancia EC2 es una máquina virtual en Azure o una instancia Compute Engine en Google Cloud.

Cada recurso de AWS reside en un lugar concreto. El servicio se divide en regiones, cada una diseñada para estar aislada de las demás, y cada región contiene varias zonas de disponibilidad. Una zona comprende uno o más centros de datos diferenciados, con suministro eléctrico, redes y conectividad redundantes, físicamente separados de las otras zonas de su región. Un recurso se crea en una región, a menudo en una sola zona, y el equipo elige el lugar teniendo en cuenta la latencia, la legislación y el precio.

El acceso a todo ello pasa por AWS Identity and Access Management, o IAM. Una cuenta comienza con un usuario root que puede hacerlo todo, e IAM añade usuarios, grupos, roles y políticas que indican qué llamada API se permite sobre

qué recurso y en qué condiciones. La mayoría de las preguntas sobre seguridad de AWS resulta ser, en el fondo, una pregunta sobre esas políticas.

Utilice el concepto en una decisión

Aplique «¿Qué es AWS?» a una decisión real. Podemos ayudarle a relacionar el concepto con el sistema que está construyendo o comprando. Servidores dimensionados para el uso real, trasladados a la nube o fuera de ella, con la factura mensual calculada de antemano.

Explore nuestros servicios Póngase en contacto →

Compruebe los supuestos detrás del término

Utilice la explicación y los trabajos enlazados para formular preguntas sobre su proyecto. Podemos examinar los supuestos con usted antes de elegir una herramienta. 20 aplicaciones Docker en Google Cloud y AWS — 20 aplicaciones en contenedores desplegadas y monitorizadas

20 aplicaciones Docker en Google Cloud y AWS Póngase en contacto →

Por qué importa

Los equipos eligen AWS por su amplitud. Un producto que necesita PostgreSQL gestionado, una cola, una red de distribución de contenido, almacenamiento de objetos y un lugar donde ejecutar contenedores puede reunirlo todo bajo una sola factura y un solo sistema de identidad, con documentación que sigue un patrón común. Esa amplitud también tiene un precio. Cada servicio tiene sus propias dimensiones de tarificación, sus propios límites y su propio rincón del lenguaje de políticas de IAM; un equipo que adopta diez servicios pasa a mantener diez pequeñas integraciones con las interfaces de Amazon. Marcharse después exige sustituirlas todas.

La segunda decisión es qué sigue a cargo del cliente. AWS publica un modelo de responsabilidad compartida y traza la frontera con dos expresiones: AWS responde de la seguridad de la nube («of»), es decir, de «el hardware, el software, las redes y las instalaciones que hacen funcionar los servicios de AWS Cloud», y el cliente de la seguridad en la nube («in»). La posición de esa frontera depende del servicio. En una instancia EC2, el cliente parchea el sistema operativo invitado, se ocupa de todos los programas instalados en él y configura el grupo de seguridad, el cortafuegos que está delante de la instancia. En S3 o DynamoDB, AWS opera el sistema y la plataforma, mientras que al cliente le corresponden los datos, sus opciones de cifrado y los permisos que deciden quién puede leerlos.

La tercera decisión es el coste, que en AWS es más una propiedad del diseño que una factura que llega después. Well-Architected Framework de Amazon define seis pilares con los que revisar una carga de trabajo: excelencia operativa, seguridad, fiabilidad, eficiencia del rendimiento, optimización de costes y sostenibilidad. El coste merece estar en esa lista porque un mismo sistema puede

construirse de forma barata o cara según decisiones de su primera semana: tamaños de instancias, número de zonas, volumen de datos que sale de la región y servicios gestionados que sustituyen a un proceso en un servidor convencional.

Cómo se aplica en la práctica

En la página de tecnologías, AWS acompaña a Google Cloud como una de las dos nubes habituales; Azure se añade donde ya opera el cliente.

Un encargo utilizó ambas nubes a la vez: veinte aplicaciones Docker se ejecutaban en Google Cloud y AWS, algunas de ellas aplicaciones de analítica basadas en R. Se desplegaban y mantenían con la misma configuración y monitorización en cada nube para que ninguna acabara convertida en un caso especial. Cuando algo fallaba, la resolución de problemas pasaba por Podman y la depuración de la orquestación por Kubernetes, y las aplicaciones analíticas se mantenían estables y reproducibles en producción en ambos lados.

Otro encargo recorrió el camino contrario. Para un cliente internacional, una configuración AWS estaba sobredimensionada y había acumulado servicios sin uso, y el coste había crecido fuera de proporción con las necesidades del negocio. El trabajo revisó qué servicios se utilizaban, eliminó los innecesarios, ajustó la capacidad restante y trasladó cargas de trabajo fuera de AWS. Esos cambios de infraestructura son el trabajo entregado que describe el registro. Este no acredita una proporción de costes en condiciones equivalentes, una medición de productividad ni una migración sin interrupciones. El ejemplo resulta útil por su método de examinar la configuración existente y cambiar lo que el negocio necesita operar, no como promesa de un ahorro determinado.

Ambos casos se reducen al mismo hábito. Un servicio de pago por uso factura todo lo que se haya activado, por lo que un entorno AWS se mantiene sano cuando alguien sigue contrastando lo que está en ejecución con lo que utiliza el negocio.

Dónde surgen los problemas

AWS rara vez pierde datos o permanece caído mucho tiempo. Los incidentes caros suelen comenzar dentro de la propia cuenta.

El usuario root hace el trabajo diario. Toda cuenta comienza con un usuario root, el correo y la contraseña con los que se abrió, con acceso sin restricciones a todos los recursos y ajustes, incluido el cierre de la cuenta. Iniciar sesión como root para las tareas habituales hace que una sola contraseña filtrada alcance todo. AWS recomienda proteger las credenciales root, añadirles autenticación multifactor y reservarlas para las pocas tareas que las requieren, mientras el trabajo diario se hace mediante inicio de sesión federado y roles.

Se filtran claves de acceso de larga duración. Un par de claves de acceso funciona hasta que alguien lo elimina, y viaja con facilidad: a los archivos ocultos de un portátil, una variable de CI, una imagen de contenedor o un commit. La lista de buenas prácticas de IAM comienza por el extremo contrario. Las personas inician sesión a través de un proveedor de identidad y reciben credenciales temporales, y las cargas de trabajo obtienen credenciales temporales de un rol IAM asociado al entorno de cómputo donde se ejecutan. Cuando una clave de larga duración sea realmente necesaria, rótela y elimine las claves, los usuarios y los roles que hayan quedado sin uso.

Se confunde una alerta de presupuesto con un freno. AWS Budgets envía una notificación cuando el gasto real o previsto supera un umbral y actualiza sus cifras hasta tres veces al día, por lo que una alerta informa de dinero que ya se ha gastado. Los recursos siguen funcionando y facturando. Budgets también puede ejecutar una acción, como aplicar una política IAM o una política de control de servicios que impida crear recursos nuevos, o actuar sobre instancias concretas EC2 o RDS. Solo lo hace cuando esa acción se ha configurado de antemano, con un rol a través del que actuar.

Todo reside en una sola zona de disponibilidad. Una única instancia con un único disco en una zona es la configuración más barata y comparte el destino de ese lugar. Las zonas existen para que un fallo de suministro eléctrico o red en una deje a las demás en funcionamiento, y la documentación de AWS recomienda distribuir una aplicación entre varias. Una base de datos importante recibe una réplica en espera en una segunda zona, y una capa web recibe instancias en al menos dos zonas, detrás de un balanceador que abarque ambas.

Un bucket abierto para una demostración sigue abierto. Los buckets S3 nuevos bloquean el acceso público de forma predeterminada, pero una política de bucket o un permiso de objeto puede cambiarlo en un minuto, y un enlace compartido con un cliente para una tarde sigue siendo público un año después. S3 Block Public Access, configurado para toda la cuenta u organización, prevalece

sobre esas políticas. Actívelo siempre que una cuenta no tenga motivo para publicar archivos y sirva los archivos públicos desde un bucket creado para ese fin.

Lecturas adicionales

- Documentación AWS — el índice de guías de usuario, referencias API y tutoriales para todos los servicios AWS.
- Responsabilidad compartida — la explicación del pilar de seguridad de Well-Architected sobre qué capas protege AWS y cuáles protege el cliente.
- Pilares del marco — las seis áreas con las que AWS pide revisar una carga de trabajo, entre ellas el coste y la fiabilidad.
- Regiones y zonas de disponibilidad AWS — cómo se aíslan las regiones y las zonas, y por qué una aplicación debería abarcar varias zonas.
- Buenas prácticas de seguridad en IAM — federación, roles, autenticación multifactor, usuario root y mínimo privilegio en una sola lista.
- Gestionar costes con AWS Budgets — presupuestos sobre gasto real y previsto, sus notificaciones y las acciones que pueden ejecutar.



Glosario

Elija según sus restricciones reales

Describa la ruta de despliegue, los riesgos operativos y quiénes se encargan de las guardias. Podemos definir el alcance de un cambio con comprobaciones, una vía de recuperación y responsabilidades claras.

Vea cuánto cuesta Póngase en contacto →

Haga práctica la terminología

Pregunte cómo se aplica «¿Qué es AWS?» a su organización. Basta un ejemplo concreto de su sistema actual para iniciar la conversación.

Explore nuestros servicios

welcome@engineer.company +45 50 10 61 84 Copenhague, Dinamarca

Llévese esta página

Tarjeta de contacto

Creado con esmero y cariño por D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Derechos de autor © 2025 – actualidad · Engineer ApS · Todos los derechos reservados.

Impreso desde https://engineer.company/es/glossary/aws/