

AWS Certified Cloud Practitioner

Domina los conceptos oficiales y habilidades clave del formato de CLF-C02, para repasar antes del examen.

Nivel: Beginner Duración: 90 min Nota de corte: 700/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Cloud Concepts

24–24%

Define the benefits of the AWS Cloud

- La propuesta de valor de AWS se resume en seis ventajas: cambiar gastos fijos por variables, aprovechar enormes economías de escala, dejar de adivinar la capacidad, ganar velocidad y agilidad, dejar de gastar en operar centros de datos y llegar a todo el mundo en minutos. Se paga solo por lo que se consume y los recursos están disponibles en minutos, no en semanas.
- La infraestructura global de AWS se organiza en regiones aisladas entre sí, cada una con varias zonas de disponibilidad. Permite desplegar en varias regiones con pocos clics para acercar las aplicaciones a los usuarios y reducir la latencia, elegir la región según requisitos legales (AWS no replica recursos entre regiones por su cuenta) y entregar contenido desde ubicaciones de borde con Amazon CloudFront.
- La alta disponibilidad se consigue repartiendo la carga entre varias zonas de disponibilidad aisladas de una región, de modo que el fallo de una ubicación no detiene la aplicación. La elasticidad evita sobreaprovisionar: los recursos crecen y se reducen con la demanda. La agilidad permite tener recursos en minutos y experimentar con poco coste y tiempo.

Identify design principles of the AWS Cloud

- El AWS Well-Architected Framework reúne prácticas recomendadas y preguntas para evaluar cargas de trabajo en seis pilares. Sus principios generales incluyen dejar de adivinar la capacidad, probar a escala de producción, automatizar, arquitecturas evolutivas, decisiones basadas en datos y game days. Las revisiones son conversaciones sin culpables, no auditorías, y AWS Well-Architected Tool las documenta.
- El marco tiene seis pilares: excelencia operativa (operar y mejorar procesos), seguridad (proteger datos, sistemas y activos), fiabilidad (funcionar de forma correcta y constante y recuperarse de fallos), eficiencia del rendimiento (usar los recursos con eficiencia a medida que cambia la demanda), optimización de costes (aportar valor al menor precio) y sostenibilidad (reducir el consumo de energía).
- Los pilares se distinguen por su objetivo: fiabilidad limita el impacto de los fallos (escalar en horizontal, recuperarse solo); eficiencia del rendimiento elige y ajusta recursos para responder bien (caché, compresión); optimización de costes busca el menor precio por valor entregado; sostenibilidad reduce la energía y los recursos por unidad de trabajo; excelencia operativa mejora la operación.

Understand the benefits of and strategies for migration to the AWS Cloud

- El AWS CAF propone un recorrido iterativo e incremental en cuatro fases: Envision (identificar oportunidades ligadas a resultados), Align (detectar carencias de capacidades), Launch (pilotos en producción) y Scale (ampliar el valor). En migraciones grandes, AWS recomienda rehost, relocate o replatform primero y modernizar después, porque AWS ofrece recursos para cada fase de la migración: Migration Evaluator crea un caso de negocio basado en datos del entorno local; el AWS Migration Acceleration Program (MAP) combina metodología, herramientas, formación, partners e inversión; AWS Professional Services y AWS Partners aportan expertos; y servicios como AWS DataSync y AWS DMS mueven archivos y bases de datos.
- El AWS CAF agrupa sus capacidades fundamentales en seis perspectivas: Business, People, Governance, Platform, Security y Operations, cada una con sus partes interesadas. Busca cuatro resultados de negocio: reducir el riesgo empresarial, mejorar el desempeño ESG, aumentar los ingresos con nuevos productos y mercados, y aumentar la eficiencia operativa.
- Las 7 R de migración son retire, retain, rehost, relocate, repurchase, replatform y refactor. Rehost traslada sin cambios; replatform añade optimizaciones, como pasar a Amazon RDS; retain deja la aplicación en origen. Para bases de datos, AWS DMS migra entre motores iguales o distintos y puede replicar cambios en curso para mantener origen y destino sincronizados hasta el corte.

Understand concepts of cloud economics

- En la economía de la nube se paga por uso, sin contratos largos ni penalizaciones al dejar de usar un servicio; se ahorra comprometiendo un uso (Savings Plans) y se paga menos por unidad cuanto más se usa. El AWS Cloud Value Framework mide el valor más allá del TCO: productividad del personal, resiliencia operativa, agilidad empresarial y sostenibilidad.
- Pasar a la nube ahorra porque se paga solo por lo que se usa: los entornos que no trabajan todo el día pueden detenerse. Además, las estrategias de migración tienen efecto en el coste: repurchase (SaaS) suele reducir mantenimiento, infraestructura y licencias, y replatform puede abaratar con servicios administrados, procesadores y almacenamiento.
- En un centro de datos propio, servidores e instalaciones son costes fijos que se pagan por adelantado y se usan o no. En AWS se convierten en costes variables: se paga solo por lo que se consume y la inversión de capital en TI puede pasar a ser gasto operativo. Así se reduce el riesgo de comprar activos que dejen de necesitarse y de tener capacidad ociosa.
- Un entorno local exige una inversión inicial en hardware, licencias de software e instalaciones, y gastos continuos de electricidad, refrigeración, personal y mantenimiento durante todo el ciclo de vida del equipo. Escalar requiere planificar, comprar e instalar hardware, que no puede reducirse después. En la nube, el proveedor mantiene la infraestructura física y se paga por uso.
- Con License Included, AWS posee la licencia del software y su coste va incluido en el precio del recurso; con BYOL reutilizas licencias que ya tienes. Las licencias por socket o por núcleo se aprovechan con EC2 Dedicated Hosts, y AWS License Manager controla su consumo y permite cambiar entre BYOL y licencias de AWS sin volver a desplegar las cargas.

2. Security and Compliance

30–30%

Understand the AWS shared responsibility model

- La seguridad y el cumplimiento se reparten entre AWS y el cliente: AWS se ocupa de la seguridad de la nube y el cliente de la seguridad en la nube. El reparto depende de los servicios elegidos, de cómo se integran y de la normativa aplicable, y se extiende a la seguridad de los controles de protección, gestión, operación y verificación de la seguridad en la nube (el cliente). Los controles se agrupan en heredados, como los físicos y ambientales; compartidos, como la gestión de parches, la de configuración y la formación; y específicos del cliente, como zonificar datos en entornos de seguridad concretos.
- El cliente es responsable de la seguridad en la nube: sus datos y su cifrado, la clasificación de activos, los permisos de IAM, la configuración de red y de security groups y, en Amazon EC2, el sistema operativo invitado con sus parches y el software instalado. También debe demostrar su propio cumplimiento normativo, porque los informes de AWS solo cubren la parte de AWS.
- AWS es responsable de la seguridad de la nube: el hardware, el software, la red y las instalaciones que ejecutan sus servicios, desde el sistema operativo del host y la capa de virtualización hasta la seguridad física. Eso incluye la alimentación, la refrigeración, el control de acceso a los centros de datos, la retirada segura de soportes y, en los controles compartidos se aplican a la infraestructura y a la capa del cliente, cada uno en su ámbito: en la gestión de parches AWS parchea su infraestructura y el cliente su sistema operativo invitado y sus aplicaciones; en la configuración ocurre lo mismo; y cada parte forma a sus propios empleados. En servicios como Amazon RDS,

Understand AWS cloud security, governance, and compliance concepts

- El gobierno en AWS combina varias piezas: AWS Organizations gestiona cuentas de forma centralizada y sus service control policies limitan los permisos máximos sin concederlos; AWS Control Tower monta una landing zone con controles según prácticas recomendadas; y AWS Config registra el historial de configuración y evalúa con reglas.
- El cifrado vuelve ilegibles los datos sin la clave de descifrado y, junto con los controles de acceso, reduce el riesgo de acceso no autorizado en reposo y en tránsito. AWS KMS crea y controla claves en módulos de seguridad de hardware gestionados por AWS, cada uso de una clave queda registrado en CloudTrail y Amazon S3 cifra por defecto los objetos nuevos.
- AWS CloudTrail registra quien hizo qué acción de API, sobre qué recurso y cuando; VPC Flow Logs captura el tráfico IP de las interfaces de red; los registros de acceso de S3 y de Elastic Load Balancing recogen solicitudes a buckets y balanceadores; CloudWatch Logs centraliza y consulta registros; y Amazon Security Lake reúne datos de seguridad de varias fuentes en un data lake con esquema OCSF.
- AWS Artifact es el portal de autoservicio para descargar bajo demanda los informes de cumplimiento de AWS (SOC, ISO, PCI) y para revisar, aceptar y seguir acuerdos como el BAA, también para toda una organización. La página AWS Services in Scope by Compliance Program indica qué servicios cubre cada programa; que un servicio no figure no impide usarlo, pero el cliente debe evaluar sus datos.
- Las obligaciones de cumplimiento dependen del país y del sector. Con las AWS Regions el cliente decide dónde se almacenan sus datos, algo clave para normas como el GDPR. AWS distingue certificaciones evaluadas por auditores externos (ISO 27001, SOC 2) de leyes como HIPAA, que no tienen certificación para proveedores cloud;

Identify AWS AWS service management capabilities Addendum.

- AWS Identity and Access Management (IAM) controla quién se autentica y qué está autorizado a hacer en una cuenta de AWS. Los roles de IAM entregan credenciales temporales, por ejemplo a las aplicaciones en EC2, en lugar de claves de larga duración. En AWS Organizations, las SCP fijan los permisos máximos de las cuentas.
- El usuario raíz se crea con la cuenta y tiene acceso completo a todos sus servicios y recursos, incluida la facturación, miembro, pero nunca concede permisos por sí sola.
- por lo que no debe usarse en el día a día. AWS recomienda protegerlo bien: usar un correo de grupo gestionado por la empresa, no compartir sus credenciales y repartir entre personas distintas el correo y el teléfono, que sirven para recuperar el acceso raíz.
- El principio de mínimo privilegio consiste en conceder solo los permisos necesarios para cada tarea, indicando acciones, recursos y condiciones. Se puede empezar con permisos amplios e ir reduciéndolos: la información de último acceso de IAM revela permisos sin usar e IAM Access Analyzer genera políticas detalladas a partir de la actividad registrada en AWS CloudTrail.
- AWS IAM Identity Center conecta a los usuarios de la plantilla, creados en el o sincronizados desde un proveedor de identidad existente, con sus cuentas y aplicaciones de AWS mediante el AWS access portal. La instancia de organización, en la cuenta de administración, es la práctica recomendada y permite usar permission sets para definir funciones de trabajo y asignarlas en muchas cuentas.
- Las claves de acceso son credenciales de larga duración para usar la CLI o la API, y AWS recomienda preferir credenciales temporales. La política de contraseñas de IAM fija complejidad y caducidad para los usuarios de IAM, pero no afecta al usuario raíz ni a las claves. AWS Secrets Manager guarda y rota secretos como credenciales de

Identify components and resources for security configuration.

- AWS ofrece servicios de seguridad gestionados para cada necesidad: AWS KMS crea y controla claves de cifrado, ACM emite y renueva certificados SSL/TLS, Amazon Macie descubre datos confidenciales en S3, Amazon Inspector busca vulnerabilidades de software y Amazon Detective los informes de investigación de causa raíz de los fallos.
- AWS Artifact almacena descargas bajo demanda de los informes de cumplimiento de AWS (SOC, PCI, ISO) y permite revisar y aceptar acuerdos con AWS. Estas certificaciones las evalúan auditores independientes, pero el cliente sigue respondiendo de su propio cumplimiento. El pilar de seguridad de Well-Architected reúne las prácticas recomendadas para diseñar cargas seguras.
- AWS WAF filtra las solicitudes HTTP(S) a recursos como CloudFront o un Application Load Balancer. AWS Shield Standard protege a todos los clientes sin cargo frente a los DDoS más comunes, y Shield Advanced amplía esa protección. Firewall Manager aplica reglas en todas las cuentas de una organización y GuardDuty detecta amenazas analizando registros.
- AWS Marketplace es un catálogo digital seleccionado donde se buscan, compran y despliegan productos de seguridad de terceros, como firewalls, detección de intrusiones o reglas para AWS WAF. Se entregan como AMI, SaaS o plantillas de CloudFormation, admiten modelos como prueba gratuita o BYOL y los cargos aparecen en la factura de AWS.
- AWS publica información de seguridad en varios sitios: el AWS Security Center (aws.amazon.com/security) reúne servicios, soluciones de partners y recursos de aprendizaje; AWS Security Blog trae novedades, ejemplos y talleres; Security Bulletins avisa de vulnerabilidades en servicios de AWS, y AWS Knowledge Center, en re:Post, responde a las preguntas más frecuentes.

3. Cloud Technology and Services

34-34%

Define methods of deploying and operating in the AWS Cloud

- En AWS se puede aprovisionar de varias formas: con plantillas de infraestructura como código (CloudFormation), subiendo el código de AWS a una Elastic Beanstalk, o usando una aplicación web o CLI para crear la consola o la CLI. Para operar servicios a escala, AWS Systems Manager, aplica parches y ejecuta comandos en AWS y en las instalaciones, y AWS CloudShell nos permite ejecutar comandos directamente en el navegador web o en la consola.
- Para crear una infraestructura de software, se puede usar AWS CloudFormation o AWS CloudFormation StackSets para crear una infraestructura de software en varias regiones.
- Para crear una infraestructura de software, se puede usar AWS CloudFormation o AWS CloudFormation StackSets para crear una infraestructura de software en varias regiones.

Identify the AWS global infrastructure

- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.

Identify AWS compute services

- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.

Identify AWS database services

- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.

Identify AWS network services

- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.

Identify AWS storage services

- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.

Identify AWS artificial intelligence and machine learning (AI/ML) services and analytics services

- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.

Identify services from other in scope AWS services categories and AWS

- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.
- La infraestructura de AWS es una zona geográfica con tipos de recursos y características de los recursos de los recursos.

4. Billing, Pricing, and Support

12-12%

Compare AWS pricing models

- EC2 ofrece varias formas de compra: On-Demand (pago por segundo sin compromiso), Savings Plans y Reserved Instances (compromiso de uno o tres años a cambio de descuento), Spot (capacidad sobrante interrumpible), Dedicated Hosts (servidor físico con visibilidad de sockets y núcleos para licencias propias), Dedicated Instances (hardware de un solo cliente) y Capacity Reservations (capacidad garantizada en una zona).
- Amazon S3 ofrece clases de almacenamiento según el patrón de acceso: S3 Standard para datos frecuentes, Intelligent-Tiering para patrones desconocidos, Standard-IA y One Zone-IA para datos poco consultados con acceso en milisegundos (One Zone-IA en una sola zona y para datos recreables) y las clases Glacier para archivo, con Deep Archive como la opción de menor coste.
- On-Demand encaja con cargas cortas o imprevisibles que no admiten interrupción. Spot es lo más barato si la carga es flexible y tolera interrupciones, como lotes o análisis. Para uso estable, los Savings Plans y las Reserved Instances dan descuento por compromiso: Compute Savings Plans sigue aplicándose al cambiar de familia o región y cubre Fargate y Lambda; Dedicated Hosts sirve para licencias propias.
- Las Reserved Instances ofrecen flexibilidad de dos formas. Por clase: las Standard dan más descuento pero no se pueden intercambiar, y las Convertible se intercambian durante el plazo por otra familia, plataforma o tenancy. Por ámbito: la regional aplica el descuento en cualquier zona de su región y a cualquier tamaño de la familia (Linux/Unix, tenancy por defecto) sin reservar capacidad; la zonal sí la reserva.
- Con la facturación consolidada de AWS Organizations, todas las cuentas cuentan como una sola a efectos de facturación: el beneficio de una Reserved Instance se aplica primero a la cuenta que la compró y lo sobrante puede aprovecharlo el uso coincidente de otras cuentas. La cuenta de administración puede desactivar ese uso compartido por cuenta o limitarlo a grupos de cuentas en las preferencias de facturación.

Understand resources for billing, budget, and cost management

- AWS Billing and Cost Management reúne la facturación: en la página Bills se descargan facturas y se ve el detalle de cada cargo, y hay páginas para pagos, métodos de pago, créditos y preferencias. Todos los titulares de cuentas tienen soporte de cuenta y facturación sin coste: ante dudas o reclamaciones de una factura se abre un caso de Account and billing en el AWS Support Center.
- La información de precios oficial está en la página de precios de cada servicio, que es la que AWS aplica al cobrar. Para consultarla mediante programación existe AWS Price List: la Query API busca precios por atributos a nivel de SKU y la Bulk API descarga archivos JSON o CSV por servicio y región. AWS Pricing Calculator usa esos datos para crear estimaciones.
- AWS Organizations gestiona de forma centralizada varias cuentas de AWS: permite crearlas mediante programación, agruparlas en unidades organizativas (OUs) y aplicar políticas como las service control policies (SCPs), que fijan los permisos máximos de las cuentas miembro. También simplifica la facturación con un único método de pago y una factura consolidada para todas las cuentas.
- Una cost allocation tag es una etiqueta clave-valor de un recurso que AWS usa para organizar los costes por categorías de negocio, como centro de coste, aplicación o propietario. Para que aparezca en Cost Explorer y en los informes hay que activarla en la consola de Billing and Cost Management; en una organización solo lo puede hacer la cuenta de administración.
- AWS Budgets fija importes de coste o uso, o umbrales de utilización y cobertura de Reserved Instances y Savings Plans, y avisa por email o Amazon SNS cuando el gasto real o previsto los supera; también puede ejecutar acciones como aplicar una política de IAM. AWS Cost Explorer analiza los costes y el uso históricos con gráficos, filtros y agrupaciones, muestra tendencias y prevé el gasto futuro.

Identify AWS technical resources and AWS Support options

- Los sitios oficiales de AWS reúnen recursos con fines distintos: AWS Solutions Library ofrece soluciones y guías revisadas por arquitectos de AWS, con código desplegable; AWS Decision Guides comparan servicios y explican los criterios para elegir; y AWS Architecture Center publica arquitecturas de referencia y el marco AWS Well-Architected.
- AWS ofrece Basic Support a todos los clientes y tres planes de pago: Business Support+, con acceso 24/7 a ingenieros, soporte de software de terceros y la AWS Support API; Enterprise Support, que suma un Technical Account Manager designado; y Unified Operations, para cargas de misión crítica, con Domain Specialist Engineers designados, monitorización 24/7 e Incident Management Engineers.
- La AWS Partner Network (APN) es la comunidad global de organizaciones que usan tecnologías, programas y herramientas de AWS para crear soluciones y servicios. Los ISV desarrollan software que se ejecuta en AWS (Software Path) y los integradores de sistemas prestan servicios de consultoría, profesionales o gestionados (Services Path). Los clientes los encuentran con AWS Partner Solutions Finder.
- AWS Support Center es la consola para crear y gestionar casos de soporte. Todos los clientes pueden abrir casos de cuenta y facturación y solicitudes de aumento de cuotas de servicio; los casos técnicos requieren un plan de pago. Los usuarios de IAM no tienen acceso por defecto: hay que concederles permisos, por ejemplo con la política administrada AWSSupportAccess.
- La documentación de cada servicio (guías del usuario, referencias de API y de CLI) está en docs.aws.amazon.com. Los whitepapers, guías de decisión y diagramas de arquitectura están en la página AWS Whitepapers & Guides, que incluye el resumen Overview of Amazon Web Services. Los anuncios aparecen en What's New with AWS y los artículos técnicos, en AWS Blogs.