AWS CERTIFIED CLOUD PRACTITIONER · CLF-C02

AWS Cloud Practitioner — Field Notes

Conceptos esenciales explicados para comprender, no solamente memorizar.

6 CONCEPTOS | EXPLICACIÓN + EJEMPLO + COMPARACIÓN + ERROR FRECUENTE + PREGUNTA | NOTAS DE PREPARACIÓN — JULIAN

Este documento no es material oficial de AWS. Es un resumen de estudio propio, contrastado con la documentación pública de AWS. Para el temario completo y vigente del examen, consultá la guía oficial CLF-C02.

CONCEPTO 01

Infraestructura global: Regiones, Availability Zones y Edge Locations

EXPLICACIÓN SIMPLE

Una **Región** es un área geográfica con varios centros de datos independientes. Cada **Availability Zone (AZ)** es uno o más centros de datos con energía, refrigeración y red propias, aislados de fallas en otras AZs pero unidos por redes de baja latencia. Una **Edge Location** es un punto de presencia más chico y más cercano al usuario final, usado para entregar contenido o resolver DNS — no para alojar tu infraestructura.

EJEMPLO PRÁCTICO

Distribuís instancias EC2 entre `us-east-1a` y `us-east-1b` para que un corte eléctrico en una AZ no tire abajo la aplicación. Amazon CloudFront, en cambio, usa Edge Locations en todo el mundo para servir contenido estático cerca del usuario, sin mover tu infraestructura de lugar.

COMPARACIÓN ÚTIL

Región: dónde viven tus recursos. AZ: cómo los repartís para tolerar fallas. Edge Location: cómo acercás contenido al usuario, sin relocalizar nada.

ERROR FRECUENTE

Confundir una Edge Location con "una AZ más chica". Resuelven problemas distintos: resiliencia (AZ) contra latencia de entrega de contenido (Edge Location).

PARA COMPROBAR

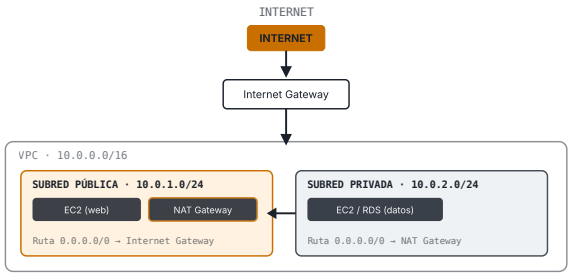
¿Qué diferencia hay entre desplegar en varias AZs y usar una Edge Location vía CloudFront?

CONCEPTO 02

Networking: VPC, subred pública/privada, Internet Gateway y NAT Gateway

EXPLICACIÓN SIMPLE

Una **VPC** es una red privada y aislada dentro de AWS. Dentro de ella, una **subred pública** tiene una ruta directa a un **Internet Gateway (IGW)**. Una **subred privada** no tiene esa ruta. Si un recurso privado necesita salir a internet, lo hace a través de un **NAT Gateway**, que vive en una subred pública.



Pública: ruta directa a un Internet Gateway. Privada: sale a internet vía el NAT Gateway que vive en la subred pública — nunca al revés.

EJEMPLO PRÁCTICO

El servidor web que recibe tráfico de usuarios va en la subred pública. La base de datos que ese servidor consulta va en la subred privada, sin IP pública, protegida de accesos directos desde internet.

COMPARACIÓN ÚTIL

El Internet Gateway habilita tráfico entrante y saliente para recursos con IP pública. El NAT Gateway solo habilita tráfico saliente iniciado desde adentro — nunca conexiones iniciadas desde internet hacia la subred privada.

ERROR FRECUENTE

Creer que el NAT Gateway "agrega seguridad". Su función es habilitar salida a internet sin exponer la subred privada a tráfico entrante; el control de acceso corre por cuenta de los Security Groups y las Network ACLs.

PARA COMPROBAR

¿Por qué una base de datos en una subred privada puede descargar un parche de seguridad, pero nadie desde internet puede conectarse directamente a ella?

CONCEPTO 03

Modelo de responsabilidad compartida

EXPLICACIÓN SIMPLE

AWS es responsable de la seguridad **de** la nube: infraestructura física, hardware, virtualización y red global. El cliente es responsable de la seguridad **en** la nube: cómo configura sus recursos, cómo gestiona identidades y permisos (IAM), cómo cifra sus datos y, cuando aplica, cómo mantiene el sistema operativo.

EJEMPLO PRÁCTICO

AWS garantiza que el hardware del datacenter esté físicamente protegido. El cliente es quien decide si un bucket de S3 es público o privado, y quién tiene permiso para leerlo.

COMPARACIÓN ÚTIL

En servicios administrados (Lambda, RDS) AWS asume más responsabilidad operativa — por ejemplo, los parches del motor de base de datos. En EC2, el cliente administra el sistema operativo, así que su porción de responsabilidad es mayor.

ERROR FRECUENTE

Asumir que "está en AWS" significa que todo riesgo de seguridad es de AWS. Una mala configuración de permisos siempre es responsabilidad del cliente.

PARA COMPROBAR

Si un bucket de S3 queda expuesto públicamente por una configuración incorrecta, ¿de quién es la responsabilidad según el modelo?

CONCEPTO 04

EC2, Lambda y contenedores: cómo elegir

EXPLICACIÓN SIMPLE

EC2 son servidores virtuales que el cliente administra (sistema operativo, parches, escalado). **AWS Lambda** ejecuta código sin administrar servidores, cobra por invocación y duración, y escala automáticamente. Los **contenedores** (Amazon ECS o EKS) empaquetan una aplicación con sus dependencias; corren sobre EC2 (el cliente administra los servidores) o sobre **Fargate** (AWS administra la infraestructura de cómputo).

EJEMPLO PRÁCTICO

Procesar una imagen apenas se sube a S3: buen caso para Lambda. Varios microservicios corriendo todo el tiempo: suele encajar mejor en contenedores. Una aplicación con requerimientos específicos de sistema operativo: puede necesitar EC2.

COMPARACIÓN ÚTIL

Control total del servidor → EC2. Cero administración, eventos puntuales → Lambda. Empaquetado consistente de la app, con o sin administrar el servidor → contenedores, con EC2 o con Fargate.

ERROR FRECUENTE

Asumir que Lambda siempre es más barato. Para cargas constantes y predecibles, EC2 o contenedores pueden salir más económicos que pagar por cada invocación.

PARA COMPROBAR

¿Qué elegirías para un proceso que corre de forma continua las 24 horas, y por qué probablemente no sea Lambda?

CONCEPTO 05

S3, EBS, EFS y las principales bases de datos

EXPLICACIÓN SIMPLE

Amazon S3 es almacenamiento de objetos accesible por red, sin estructura de sistema de archivos. **Amazon EBS** es un volumen de bloques que se adjunta a una sola instancia EC2 a la vez, como un disco virtual. **Amazon EFS** es un sistema de archivos compartido que varias instancias EC2 pueden montar al mismo tiempo. Para datos estructurados: **RDS** ofrece bases relacionales administradas, y **DynamoDB** una base NoSQL totalmente administrada y de alta escala.

EJEMPLO PRÁCTICO

Fotos de perfil de usuarios → S3. El disco del sistema operativo de una instancia → EBS. Una carpeta que varias instancias web leen y escriben a la vez → EFS. El catálogo de un e-commerce con relaciones entre tablas → RDS. Datos de sesión con lecturas y escrituras masivas y baja latencia → DynamoDB.

COMPARACIÓN ÚTIL

¿Un solo servidor necesita un disco? EBS. ¿Varios servidores necesitan compartir archivos? EFS. ¿Es un archivo que se accede por URL o API, no un disco? S3.

ERROR FRECUENTE

Intentar montar un mismo volumen EBS en varias instancias EC2 a la vez. EBS está pensado para una sola instancia; para compartir archivos entre varias, la herramienta correcta es EFS.

PARA COMPROBAR

¿Por qué EBS no es la opción correcta si tres instancias EC2 necesitan leer y escribir sobre los mismos archivos al mismo tiempo?

CONCEPTO 06

Costos, observabilidad y seguridad

EXPLICACIÓN SIMPLE	**AWS Cost Explorer** visualiza y analiza el gasto histórico. **AWS Budgets** define límites y alertas antes de que el gasto se salga de control. **Amazon CloudWatch** centraliza métricas, logs y alarmas para observar el comportamiento de los recursos. **AWS IAM** controla quién puede hacer qué, mediante usuarios, grupos, roles y políticas, siguiendo el principio de menor privilegio.
EJEMPLO PRÁCTICO	Una alarma en Budgets avisa si el gasto mensual supera un monto definido. CloudWatch indica si una instancia EC2 tiene uso de CPU anormalmente alto. Un rol de IAM específico le da a una aplicación acceso solo al bucket de S3 que necesita, nada más.
COMPARACIÓN ÚTIL	Cost Explorer mira hacia atrás (qué gasté y por qué). Budgets mira hacia adelante (qué no quiero superar). CloudWatch observa el comportamiento técnico. IAM decide quién puede actuar sobre qué recurso.
ERROR FRECUENTE	Usar las credenciales de la cuenta raíz (root) para el trabajo diario, en vez de crear usuarios o roles de IAM con permisos acotados a lo que realmente necesitan.
PARA COMPROBAR	**¿Qué herramienta usarías para que te avisen antes de gastar de más, y cuál para entender por qué una instancia está lenta?**

Learning is better when shared.

Estas notas resumen conceptos de nivel AWS Certified Cloud Practitioner (CLF-C02) con fines de estudio y difusión. No reproducen preguntas de examen reales, filtradas ni confidenciales, y no son material oficial de AWS. Fuente de referencia: guía oficial del examen CLF-C02.