SOA-C03 · CHEAT SHEET · CERTIFYDECK

AWS Certified CloudOps Engineer - Associate

Dominios, pesos oficiales y habilidades clave del temario de SOA-C03, para repasar antes del examen.

Nivel: Intermediate (Associate) Duración: 130 min Nota de corte: 720/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. Monitoring, Logging, Analysis, Remediation, and Performance Optimization 22–22%

Implement metrics, alarms, and filters by using AWS monitoring and logging services

- Cada carga de trabajo tiene su herramienta: Lambda Insights da métricas de sistema y arranques en frío de Lambda, el registro de invocaciones de Bedrock guarda peticiones y respuestas, y los recopiladores administrados de Amazon Managed Service for Prometheus extraen métricas de EKS sin agentes. CloudTrail no registra eventos de datos (como DeleteObject en S3) si no se activan; los filtros de métricas convierten registros en métricas con alarma.
- El agente de CloudWatch recopila métricas del sistema invitado (memoria, disco) y registros, con un rol que tenga CloudWatchAgentServerPolicy. En flotas, la configuración se guarda en Parameter Store y se aplica con AmazonCloudWatch-ManageAgent; tras editarla hay que usar fetch-config. En ECS sobre EC2 se despliega como servicio daemon en EKS con DaemonSet.
- Las alarmas pueden notificar a SNS, invocar Lambda (con una política de recursos para lambda.alarms.cloud-watch.amazonaws.com), ejecutar acciones de EC2 y Auto Scaling y crear OpsItems; para otros destinos se usan sus eventos en EventBridge. Las alarmas compuestas combinan estados con AND, OR y NOT, no lanzan Auto Scaling y las de CloudWatch suprimen notificaciones y acciones si faltan datos. Los proveedores (propiedades accountId y region) si cada cuenta comparte sus datos con la de supervisión. Para registros y alarmas entre cuentas en una región se usa la observabilidad entre cuentas. Las variables permiten cambiar, por ejemplo, de función de Lambda, y un tema publicar en SNS sus propios correos, pulsaciones de RDS, notificaciones de Auto Scaling (EC2_INSTANCE_LAUNCH_ERROR), notificaciones de eventos de S3 y el administrador de alertas de Amazon Managed Service for Prometheus. El tema necesita una política que permita publicar a la entidad principal del servicio y, si está cifrado, una clave administrada por el cliente que le conceda kms:GenerateDataKey* y kms:Decrypt.

Identify and remediate issues by using monitoring and availability metrics

- La detección de anomalías de CloudWatch compara una métrica con su banda esperada según la estacionalidad. Las alarmas de EC2 reinician la instancia ante fallos de la comprobación de instancia y la recuperan solo con StatusCheckFailed_System. AWS Config corrige recursos con manuales de Automation, y EventBridge puede lanzar un manual si se rellenan sus parámetros obligatorios. AWS DevOps Agent investiga incidentes y propone mitigaciones.
- EventBridge enruta eventos con reglas por bus; los de CloudTrail solo llegan al bus predeterminado, los de servicios globales como IAM solo a us-east-1 y los de solo lectura exigen el estado ENABLED_WITH_ALL_CLOUD-TRAIL_MANAGEMENT_EVENTS. Los transformadores de entrada reescriben el evento, Pipes lo enriquece lla-mando a API Gateway, Lambda o Step Functions, y el programador de tareas define ventanas de mantenimiento.
- Automation de Systems Manager ejecuta manuales y de procedimientos predefinidos (como AWS-RestartEC2Instance) o personalizados, con destinos por etiqueta y controles de frecuencia (simultaneidad y umbral de errores). aws:executeScript ejecuta Python o PowerShell y aws:executeAwsApi llama a la API con reintentos automáticos; aws:approve pide aprobación por SNS. Se lanza desde la CLI o los SDK, EventBridge, AWS Config o en varias cuentas y regiones.

Implement performance optimization strategies for compute, storage, and database resources

- AWS Compute Optimizer analiza las métricas de CloudWatch y las especificaciones de EC2, grupos de Auto Scaling, Lambda, EBS o ECS en Fargate para detectar recursos mal dimensionados. La memoria exige el agente de CloudWatch con la dimensión InstanceId, y las métricas mejoradas amplían el periodo analizado. Las recomendaciones se filtran por etiquetas; en instancias T, CPUCreditBalance a cero en modo estándar limita la CPU a la referencia.
- Los volúmenes SSD (gp3, gp2, io2) sirven para cargas transaccionales limitadas por IOPS y los HDD (st1, sc1) para cargas secuenciales de alto rendimiento; gp3 no usa ráfagas y aprovisiona IOPS y rendimiento por separado. Elastic Volumes cambia tipo y rendimiento sin parar la instancia. Métricas clave: BurstBalance, VolumeQueueLength y las de IOPS y rendimiento; los discos de instancia ofrecen la latencia más baja.
- S3 Transfer Acceleration usa ubicaciones de borde para subidas rápidas a distancia mediante el punto de enlace s3-accelerate; la carga multiparte sube partes en paralelo y reintenta solo las fallidas. DataSync mueve datos de NFS, SMB u otras nubes a S3 con validación de integridad y límite de ancho de banda. El ciclo de vida de S3 transiciona objetos con arreglo a reglas de edad, Intelligent-Tiering lo adapta a accesos y políticas de ciclo de vida que mueven archivos a IA y Archive y pueden devolverlos a Standard en el primer acceso. FSx for Windows File Server sirve SMB con Active Directory, FSx for Lustre da alto rendimiento POSIX vinculado a S3 y FSx for NetApp ONTAP ofrece NFS, SMB y iSCSI con deduplicación y capas de rendimiento.
- Con Enhanced Database Insights mide la carga de la base de datos en sesiones activas medias y la desglosa por SQL, esperas, hosts o usuarios; con retención de pago genera recomendaciones proactivas. Enhanced Monitoring muestra procesos del sistema operativo. RDS Proxy agrupa y reutiliza conexiones (útil con Lambda) y solo se asocia a la instancia de escritura. Las réplicas de lectura descargan lecturas y ReplicaLag mide su retraso.

2. Reliability and Business Continuity

22–22%

Implement scalability and elasticity

- Amazon EC2 Auto Scaling ofrece seguimiento de destino (con métricas proporcionales al número de instancias, como ALBRequestCountPerTarget o el trabajo pendiente de SQS por instancia), escalado por pasos, acciones programadas y escalado predictivo para tráfico cíclico. Los warm pools y el calentamiento de instancias suavizan los arranques largos, y los enlaces de ciclo de vida permiten actuar antes de lanzar o terminar.
- En CloudFront, la política de caché define la clave de caché y los TTL, y la política de solicitudes al origen envía datos al origen sin tocar esa clave; Origin Shield añade una capa que consolida peticiones. ElastiCache usa estrategias como la carga diferida, la escritura simultánea y el TTL, y escala réplicas o particiones con Application Auto Scaling; DAX cachea lecturas eventualmente coherentes de DynamoDB.
- RDS amplía el almacenamiento automáticamente hasta un umbral máximo y escala lecturas con réplicas de lectura; RDS Proxy agrupa conexiones ante picos. Aurora Auto Scaling añade o quita réplicas (no actúa sobre el escritor) y Aurora Serverless escala el cómputo de cada instancia en un rango. DynamoDB ofrece modo bajo demanda o aprovisionado con escalado automático para tablas e índices secundarios globales.

Implement highly available and resilient environments

- Un Application Load Balancer solo envía tráfico a destinos que superan su comprobación de estado; los códigos de motivo (Target.Timeout, Target.ResponseCodeMismatch) orientan el diagnóstico y los grupos de seguridad y ACL de red deben permitir el puerto de comprobación. Route 53 comprueba puntos de enlace, otras comprobaciones (calculadas) o alarmas de CloudWatch, y Evaluate Target Health hace que los alias respeten el estado.
- Una implementación Multi-AZ de instancia de RDS mantiene una réplica en espera síncrona que no atiende lecturas; el clúster Multi-AZ añade dos lectores legibles. Aurora promueve réplicas de otras zonas y su punto de enlace del clúster sigue al principal. ElastiCache Multi-AZ exige réplicas en otra zona, EFS Regional guarda datos en varias zonas y el desvío zonal automático de ARC aparta el tráfico de una zona con problemas.

Implement backup and restore strategies

- AWS Backup centraliza las copias de EC2, EBS, RDS, DynamoDB, EFS, FSx o S3 con planes que fijan programación, retención y copias a otras regiones o cuentas, y asigna recursos por etiquetas, siempre que el servicio tenga activada la participación (opt-in). Vault Lock en modo de cumplimiento hace las copias inmutables, y Data Lifecycle Manager automatiza solo instantáneas de EBS y AMI.
- La restauración a un momento dado de RDS, Aurora y DynamoDB siempre crea una instancia, clúster o tabla nuevos, con grupos de parámetros y ajustes que hay que revisar después. El retroceso de Aurora MySQL rebobina el mismo clúster en minutos, un clon de Aurora da una copia rápida que ocupa poco, y la replicación entre regiones de las copias automatizadas de RDS permite restaurar a un momento dado en otra región.
- Con el control de versiones de S3, una sobrescritura crea una versión nueva y un DELETE simple añade un marcador de eliminación; un bucket con versiones solo se puede suspender, y las reglas NoncurrentVersionExpiration limpian las versiones antiguas. En FSx for Windows File Server hay que activar las instantáneas de volumen (shadow copies), y en FSx for ONTAP los usuarios recuperan archivos desde el directorio .snapshot.
- Copia de seguridad y restauración necesita infraestructura como código para cumplir el RTO; la luz piloto mantiene los datos replicados y obliga a encender y escalar los servidores; la espera semiactiva solo hay que escalarla; activo/activo sirve tráfico en varias regiones. Para conmutar, Route 53 y Global Accelerator usan comprobaciones de estado, y ARC aporta controles de enrutamiento, cambio zonal y Region switch.

3. Deployment, Provisioning, and Automation

22–22%

Provision and maintain cloud resources

- EC2 Image Builder automatiza AMI e imágenes de contenedor con canalizaciones programadas, recetas, componentes de compilación y prueba, configuración de infraestructura y distribución a regiones, cuentas y plantillas de lanzamiento; sus políticas de ciclo de vida retiran versiones antiguas. En EC2 se puede marcar una AMI como obsoleta o protegerla contra la anulación del registro, y ECR ofrece etiquetas inmutables y análisis al subir.
- Los conjuntos de cambios muestran antes de ejecutar si un recurso se modificará o se sustituirá; la protección contra la terminación impide borrar la pila, la política de pila protege recursos en las actualizaciones y DeletionPolicy decide qué queda al eliminarla. En AWS CDK, cdk diff compara plantillas y cdk drift detecta cambios hechos fuera de CloudFormation.
- Los fallos de despliegue se diagnostican con el motivo del evento de la pila: UPDATE_ROLLBACK_FAILED se arregla corrigiendo la causa (por ejemplo, enviando señales con signal-resource) y continuando la reversión, y los nombres personalizados de IAM exigen CAPABILITY_NAMED_IAM. Cada subred reserva cinco direcciones, y con awsvpc o EKS cada tarea o Pod consume una IP, así que las subredes pequeñas se agotan.
- StackSets despliega una plantilla en varias cuentas y regiones: con permisos administrados por el servicio usa AWS Organizations, crea los roles y admite implementaciones automáticas, pero no despliega en la cuenta de administración; con permisos autoadministrados se crean roles de administración y ejecución. AWS RAM es regional y comparte recursos como subredes o puertas de enlace de tránsito sin invitaciones dentro de la organización.
- Las estrategias de despliegue van desde la actualización en el sitio o continua hasta azul/verde, canary y lineal. En ECS, minimumHealthyPercent y maximumPercent marcan cuántas tareas se paran o arrancan y el interruptor de circuito revierte si no arrancan; en Auto Scaling, la actualización de instancias admite puntos de control y reversión automática con alarmas; CodeDeploy y los alias ponderados trasladan tráfico en Lambda.

Automate the management of existing resources

- Systems Manager automatiza la operación: State Manager mantiene un estado definido e incluye nodos nuevos, Maintenance Windows ejecuta tareas por prioridad dentro de un horario, Run Command actúa a escala con max-concurrency y max-errors, y Automation ejecuta manuales con rol asumido, aprobaciones, supervisión de alarmas y despliegue en varias cuentas y regiones. Las políticas de parches de Quick Setup cubren toda la organización.
- Las notificaciones de eventos de S3 envían eventos a SNS, SQS estándar, Lambda o EventBridge; los destinos necesitan una política que permita publicar a S3 y los filtros no pueden solaparse. Las reglas de EventBridge filtran con patrones, transforman la entrada, usan colas de mensajes fallidos y reciben eventos de otras cuentas. AWS DevOps Agent investiga incidentes de forma automática y propone causa raíz y mitigación.

4. Security and Compliance

16–16%

Implement and manage security and compliance tools and policies

- La política de contraseñas aplica las nuevas reglas de longitud en el siguiente cambio, pero la caducidad de inmediato. aws:MultiFactorAuthPresent solo existe con credenciales temporales (GetSessionToken o AssumeRole). [illegible] -message descifra [illegible] Regiones [illegible] y cada [illegible] conexión [illegible] de Config activada y ofrece una puntuación de conformidad. Los agregadores dan una vista de solo lectura de varias cuentas y Regiones, y Control Tower limita Regiones con sus controles de denegación para la zona de aterrizaje o por OU.
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Implement strategies to protect data and infrastructure

- Un esquema de clasificación define niveles de sensibilidad y los controles de cada nivel; se aplica con etiquetas normalizadas mediante políticas de etiquetas de AWS Organizations y con cuentas separadas por nivel. Amazon [illegible] CloudFront el certificado debe estar en [illegible] vicio, por ejemplo con [illegible] presión los archivan sin enviarlos a Security Hub CSPM; las reglas de automatización de Security Hub CSPM cambian gravedad o estado al ingerirlos, y Amazon Inspector exporta informes CSV o JSON a S3 cifrados con una clave de KMS.
- [illegible]
- [illegible]
- [illegible]
- [illegible]

5. Networking and Content Delivery

18–18%

Implement and optimize networking features and connectivity

- Los grupos de seguridad tienen estado y solo admiten reglas que permiten; las ACL de red no tienen estado, se evalúan por número ascendente y necesitan reglas para los puertos efímeros de la respuesta. Una subred es pública [illegible] prefijos; los de interfaz crean interfaces de red cuyo [illegible] Load [illegible] WAF van a destinos cuyo nombre empieza [illegible] cobran por hora y por GB. Una NAT por zona evita la transferencia entre zonas, CloudFront reduce la transferencia de datos con caché en el borde, y Public IP Insights de IPAM ayuda a liberar IP elásticas sin usar.
- [illegible]
- [illegible]
- [illegible]

Configure domains, DNS services, and content delivery

- Route 53 VPC Resolver responde en la dirección de la VPC más dos; los puntos de enlace de entrada reciben consultas de la red local y los de salida, con reglas de reenvío por dominio, las envían hacia ella. Una regla de [illegible] registro predeterminado para ubicaciones [illegible] NS. Global Accelerator ofrece IP estáticas anycast para TCP y UDP, controles de tráfico por región, pesos por punto de enlace y afinidad de cliente por IP de origen.
- [illegible]
- [illegible]

Troubleshoot network connectivity issues

- Las reglas de una ACL de red se evalúan desde el número más bajo y los grupos de seguridad solo admiten reglas de permiso. Una NAT pública necesita una subred con ruta a la puerta de enlace de internet y cierra conexiones [illegible] redes; [illegible] 504 con target_processing_time -1 [illegible] sin dividir la caché. Con un TTL mínimo mayor que 0, CloudFront ignora no-cache y no-store. Para archivos que cambian a menudo se recomiendan nombres con versión; las invalidaciones distinguen mayúsculas y deben cubrir las cadenas de consulta.
- Con Site-to-Site VPN, la tabla de rutas necesita una ruta hacia la puerta de enlace privada virtual, que la propagación añade sola, y una ruta estática con el mismo CIDR tiene prioridad. Los puntos de enlace de tipo gateway no sirven [illegible] Network Synthetic Monitor (sondas sin agentes hacia destinos locales). También hay métricas como TunnelState de VPN, ErrorPortAllocation de NAT, PacketDropCountBlackhole de la puerta de enlace de tránsito y los contadores ethtool del agente.
- [illegible]