DOP-C02 · CHEAT SHEET · CERTIFYDECK

AWS Certified DevOps Engineer – Professional

Palabras pesadas oficiales y capacidades clave del temario de DOP-C02, para repasar antes de examen.

Nivel: Advanced (Professional) Duración: 180 min Nota de corte: 750/1000 Fuente: guía de estudio oficial de Microsoft Learn

1. SDLC Automation

22–22%

Implement CI/CD pipelines

- CodeArtifact recomienda un único repositorio por dominio con la conexión externa al registro público y que el resto lo use como repositorio ascendente; el acceso entre cuentas exige política de dominio y de repositorio. En Amazon ECR, las políticas de ciclo de vida expiran imágenes por prioridad de reglas, la replicación entre cuentas solo requiere política de registro en el destino y la caché de extracción sincroniza registros como Docker Hub.
- Las canalizaciones V2 de CodePipeline con conexiones de AWS CodeConnections admiten disparadores por envío (ramas, rutas de archivo y etiquetas Git) y por solicitudes de incorporación de cambios; los filtros de un mismo tipo se combinan con AND y las exclusiones prevalecen. El formato CODEBUILD_CLONE_REF entrega un clon completo a CodeBuild, y Git en el CloudFormation mantiene una pila sincronizada con un repositorio.
- CodeBuild ejecuta las fases install, pre_build, build y post_build del buildspec; la caché de Amazon S3 se comparte entre hosts y admite claves dinámicas, mientras que la caché local solo vale para el mismo host y no funciona con VPC. Las compilaciones en VPC usan subredes privadas con una puerta de enlace NAT. Docker exige el modo privilegiado y exported-variables pasa valores a las acciones siguientes de CodePipeline.
- CodeBuild obtiene secretos con las secciones parameter-store y secrets-manager del buildspec o con variables PARAMETER_STORE y SECRETS_MANAGER, nunca PLAINTEXT. CloudFormation usa referencias dinámicas secretsmanager (otras cuentas con el ARN completo) y ssm-secure (solo la misma cuenta). El acceso entre cuentas exige política de recursos y una clave KMS del cliente, y ECS inyecta el secreto al iniciar la tarea.
- CodeDeploy ofrece despliegues in situ y azul/verde con configuraciones canario, lineales y todo a la vez para ECS y Lambda, y revierte automáticamente al fallar o al activarse una alarma. ECS tiene azul/verde nativo con tráfico de prueba, enlaces de ciclo de vida y tiempo de estabilización; Elastic Beanstalk ofrece rolling, inmutable y división de tráfico, y AWS SAM automatiza despliegues graduales de Lambda.

Integrate automated testing into CI/CD pipelines

- CodeBuild inicia compilaciones con webhooks de GitHub, GitLab y Bitbucket filtrados por eventos de solicitudes, BASE_REF o FILE_PATH, y su política de compilación de solicitudes puede exigir aprobación por comentario. CodePipeline V2 admite disparadores de solicitudes y el modo PARALLEL, y en CodeCommit las reglas de EventBridge y las plantillas de reglas de aprobación controlan pruebas y fusiones.
- Distributed Load Testing on AWS ejecuta pruebas de carga con JMeter, k6 o Locust en Fargate en varias Regiones sin servidores que gestionar. AWS FIS ejecuta experimentos con acciones, destinos por etiquetas y condiciones de parada basadas en alarmas; los canarios de CloudWatch Synthetics miden disponibilidad y latencia según un horario, y los lotes de CodeBuild reparten pruebas entre entornos aislados.
- En ECS, la comprobación de estado del contenedor ejecuta un comando cuyo código de salida 0 indica éxito y cualquier otro, fallo; solo se supervisan las comprobaciones definidas en la definición de tarea y CMD-SHELL permite operadores de shell. cfn-signal envía con -e $? el código de salida de cfn-init a la política de creación, y una acción de Lambda en CodePipeline informa del resultado con PutJobSuccessResult o PutJobFailureResult.
- CodeBuild crea informes de pruebas (JUnit XML, NUnit, TestNG, Cucumber JSON, Visual Studio TRX) y de cobertura (JaCoCo XML, SimpleCov, Clover, Cobertura, LCOV) desde la sección reports del buildspec. Un nombre de grupo crea uno con el prefijo del proyecto y un ARN reutiliza uno existente; el rol necesita BatchPutTestCases y BatchPutCodeCoverages, y los archivos pueden exportarse a S3.
- CodePipeline invoca servicios de AWS para probar con acciones administradas: la acción de Lambda debe cerrar el trabajo con PutJobSuccessResult o PutJobFailureResult (con continuationToken para procesos largos), la de Step Functions inicia una máquina de estados y, si es Standard, devuelve su salida como artefacto, e InspectorScan falla según umbrales de gravedad. CodeBuild publica informes de pruebas y cobertura desde la sección reports.

Build and manage artifacts

- En CodeArtifact se recomienda un repositorio por dominio con la conexión externa al registro público y el resto configurados con él como upstream; los controles de origen (Publish/Upstream) evitan la sustitución de dependencias. En ECR, la replicación entre cuentas exige una política del registro en el destino, el destino se configura con plantillas de creación de repositorios y la caché de extracción sincroniza registros como Docker Hub.
- CodeBuild genera artefactos según la especificación de compilación: artifacts y secondary-artifacts para varias salidas, exported-variables para pasar valores a CodePipeline y caché con claves dinámicas en S3. Las compilaciones por lotes (graph, list, matrix, fanout) usan un rol de lotes propio. El cómputo Lambda arranca más rápido pero no admite Docker, modo privilegiado, VPC ni caché.
- EC2 Image Builder automatiza imágenes con recetas (AMI o contenedor con Dockerfile y repositorio de ECR), componentes de compilación y prueba, infraestructura temporal y distribución a Regiones y cuentas, incluida la actualización de plantillas de lanzamiento. Las canalizaciones programadas pueden ejecutarse solo si hay dependencias nuevas, amazon-inspector-cli analiza las imágenes y las políticas de ciclo de vida retiran las antiguas.

Implement deployment strategies for instance, container and serverless environments

- El acceso a repositorios de artefactos combina IAM y políticas de recursos: CodeArtifact exige codeartifact:GetAuthorizationToken y sts:GetServiceBearerToken en IAM, y para otras cuentas políticas de dominio y de repositorio, que admiten aws:PrincipalOrgID. En ECS, el rol de ejecución de tareas descarga imágenes de ECR o, con repositoryCredentials, de registros privados. Los artefactos entre cuentas requieren una clave de KMS del cliente.
- El agente de CodeDeploy solo se necesita en la plataforma EC2/On-Premises, no en ECS ni Lambda. Se instala y actualiza con el paquete de Systems Manager Distributor mediante State Manager; las instancias locales se registran con un ARN de sesión de IAM y credenciales temporales. Su archivo de configuración controla :max_revisions:, :proxy_uri: y :enable_auth_policy:, necesario con puntos de conexión de VPC.
- Los fallos de despliegue se diagnostican con los eventos y registros de cada evento del ciclo de vida. En CodeDeploy, ApplicationStop usa los scripts de la última revisión correcta (--ignore-application-stop-failures lo desbloquea), los procesos largos deben redirigirse a /dev/null y DownloadBundle falla por permisos o por un bucket en otra Región.
- Cada plataforma tiene sus métodos: Elastic Beanstalk ofrece all at once, rolling, rolling con lote adicional, inmutable, traffic splitting y azul/verde con intercambio de CNAME; CodeDeploy hace in situ o azul/verde en EC2 y canario, lineal o todo a la vez en Lambda y ECS; ECS tiene azul/verde, lineal y canario nativos con tiempo de estabilización; y API Gateway publica versiones canario en una etapa. En ECS, el disyuntor de despliegue revierte y emite eventos a EventBridge.

2. Configuration Management and IaC

17–17%

Define cloud infrastructure and reusable components to provision and manage systems throughout their lifecycle

- Las plantillas de AWS SAM usan la transformación AWS::Serverless-2016-10-31, eventos que generan la API y plantillas de políticas de mínimo privilegio; package sube los artefactos locales a S3. En CodePipeline, CHANGE_SET_REPLACE y CHANGE_SET_EXECUTE permiten revisar antes de aplicar. Las exportaciones importadas no se pueden modificar, y CDK necesita bootstrap con --trust en cada entorno de destino.
- Un StackSet despliega la misma plantilla en varias cuentas y Regiones. Con permisos administrados por el servicio, StackSets crea los roles y puede desplegar automáticamente en cuentas nuevas de una OU, pero nunca en la cuenta de administración; con permisos autoadministrados hay que crear el rol de administración y el de ejecución. La concurrencia, la tolerancia a errores y el orden de Regiones controlan el riesgo del despliegue.
- AWS AppConfig cambia la configuración y los indicadores de características sin volver a desplegar código, con validadores, despliegue gradual y reversión por alarmas. State Manager mantiene los nodos en un estado deseado y puede ejecutar playbooks de Ansible o recetas de Chef sin servidor propio. AWS Config registra el historial de configuración de los recursos y evalúa su conformidad con reglas.
- Service Catalog publica productos aprobados: la restricción de lanzamiento define el rol que asume el servicio y compartir con AWS Organizations evita importaciones. Los módulos de CloudFormation se registran como extensiones privadas versionadas en cada cuenta y Región, y se usa la versión predeterminada local. En AWS CDK, los aspectos validan todas las construcciones de un ámbito y pueden hacer fallar cdk synth.

Deploy automation to create, onboard, and secure AWS accounts in a multi-account or multi-Region environment

- Control Tower ofrece varias vías para estandarizar cuentas: Account Factory Customization aplica blueprints de Service Catalog sin canalizaciones propias, CfCT despliega plantillas, SCP y RCP sincronizadas con los eventos del ciclo de vida, y AFT aprovisiona y personaliza cuentas con Terraform y GitOps. CreateAccount de Organizations es asíncrona: hay que esperar al estado SUCCEEDED antes de usar la cuenta.
- Para gobernar cuentas existentes, registrar una OU en Control Tower inscribe todas sus cuentas; la inscripción individual exige el rol AWSControlTowerExecution y no tener recursos previos de AWS Config, salvo con inscripción automática. Organizations crea OrganizationAccountAccessRole solo en las cuentas que crea, no en las invitadas, y para habilitar todas las características cada cuenta invitada debe aceptar la solicitud.
- Las SCP nunca conceden permisos: una acción debe permitirse en todos los niveles desde la raíz hasta la cuenta, un Deny en cualquier nivel prevalece y no afectan a la cuenta de administración. Las RCP limitan el acceso de entidades externas a los recursos de las cuentas miembro, y aws:PrincipalOrgID evita enumerar cuentas. El acceso entre cuentas exige la política de confianza del rol y el permiso sts:AssumeRole en el origen.
- Los controles se aplican a escala con administradores delegados: GuardDuty es regional y se activa en todas las cuentas con la preferencia ALL, y la configuración central de Security Hub CSPM aplica políticas a varias Regiones. Los paquetes de conformidad de organización necesitan un registrador de AWS Config, los agregadores son de solo lectura y los controles proactivos de Control Tower bloquean recursos antes de crearlos.

Design and build automated solutions for complex tasks and large-scale environments

- Las políticas de parches de Quick Setup aplican análisis e instalación con calendarios distintos en todas las cuentas y Regiones de una organización; las líneas base predefinidas no se editan y hay que copiarlas para asignar niveles de conformidad. Inventory admite metadatos personalizados, la sincronización de datos de recursos los centraliza en S3 para Athena y AWS Config conserva el historial del inventario.
- Step Functions llama a casi cualquier API de AWS con integraciones de SDK, sin funciones de Lambda intermedias; los flujos Standard admiten esperas con token (.waitForTaskToken) y el tipo de flujo no se puede cambiar. El Map distribuido procesa millones de objetos de S3 en flujos secundarios, y Retry con BackoffRate y Catch gestionan los errores. En Lambda asíncrona, los destinos en caso de error guardan el evento y la respuesta.
- State Manager mantiene los nodos en el estado deseado con asociaciones: un documento SSM, unos destinos (etiquetas, grupos de recursos o todos los nodos) y una programación; los nodos nuevos que reciben la etiqueta se configuran al momento. Con AWS-ApplyAnsiblePlaybooks, AWS-ApplyChefRecipes o AWS-ApplyDSCMofs se reutilizan playbooks, recetas o MOF, y la simultaneidad y el umbral de errores controlan el despliegue.
- Patch Manager aplica líneas base de parches con reglas de aprobación y listas de parches rechazados, y una política de parches de Quick Setup cubre todas las cuentas y Regiones de la organización. Compliance muestra el estado de parches y asociaciones; EventBridge puede corregir con AWS-RefreshAssociation o AWS-RunPatch-Baseline, y la sincronización de datos de recursos lleva los datos a S3 para Athena.

3. Resilient Cloud Solutions

15–15%

Implement highly available solutions to meet resilience and business requirements

- El análisis de impacto en el negocio fija cuántos datos se pueden perder (RPO) y cuánto puede tardar la recuperación (RTO); con esos objetivos se elige entre copia de seguridad y restauración, luz piloto, espera semiactiva o activo-activo, de menor a mayor coste. AWS Resilience Hub guarda los objetivos en políticas de resiliencia y evalúa si la aplicación los cumple, también desde la canalización.
- Un punto único de error es cualquier componente que solo existe en una instancia o en una zona: una puerta de enlace NAT compartida, un nodo de caché sin réplicas, una función Lambda con una sola subred o archivos en un volumen EBS. Se corrige con un recurso por zona, réplicas con Multi-AZ, subredes en varias zonas, almacenamiento regional como Amazon EFS y grupos de Auto Scaling en varias zonas.
- Varios servicios replican entre Regiones de forma administrada: las tablas globales de DynamoDB aceptan lecturas y escrituras en cada réplica, RDS admite réplicas de lectura entre Regiones que se promueven a instancia independiente, y S3 replica objetos nuevos con versiones habilitadas y los existentes con Batch Replication. CloudFront conmuta a un origen secundario, pero solo en solicitudes GET, HEAD y OPTIONS.
- Un equilibrador solo envía tráfico a las zonas habilitadas, cada una con su nodo. El equilibrio entre zonas siempre está activo en el nivel del Application Load Balancer, se puede desactivar en el grupo de destino y viene desactivado en los Network Load Balancer. Los umbrales de estado del grupo de destino retiran una zona del DNS, y las comprobaciones ELB del grupo de Auto Scaling sustituyen las instancias no saludables.
- Para reducir el tiempo de inactividad se elige el mecanismo según el caso: el switchover de Aurora Global Database cambia de Región sin pérdida de datos, las implementaciones azul/verde de RDS actualizan el motor sin cambiar la aplicación, Route 53 conmuta entre Regiones con registros de conmutación y Evaluate target health, y zonal autoshift de ARC aparta el tráfico de una zona con capacidad preescalada y ejecuciones de práctica.

Implement solutions that are scalable to meet business requirements

- Los problemas de escalado suelen venir de la métrica o del arranque: las instancias con arranques muy largos se sirven de un grupo de calentamiento, el calentamiento predeterminado evita que las instancias nuevas distorsionen la métrica, y las colas de SQS se escalan con el atraso por instancia calculado con metric math. En Lambda, la simultaneidad reservada es a la vez mínimo y máximo, así que un valor bajo provoca limitaciones.
- El escalado predictivo se adelanta a patrones diarios o semanales, las acciones programadas cubren eventos de hora conocida y conviven con el seguimiento de destino dentro del mínimo y el máximo. En caché, DAX da lecturas de microsegundos con la API de DynamoDB, y la caché de etapa de API Gateway necesita claves de caché, por ejemplo cadenas de consulta, para separar las respuestas.
- En ECS, un proveedor de capacidad de grupo de Auto Scaling con escalado administrado añade instancias según la capacidad que piden las tareas, y Service Auto Scaling ajusta el número de tareas; FARGATE y FARGATE_SPOT se combinan con base y pesos. En EKS, el Horizontal Pod Autoscaler necesita Metrics Server, y EKS Auto Mode crea y consolida nodos sin gestionar Karpenter.
- Para escalar en varias Regiones, Route 53 con registros de latencia envía a cada usuario a la Región más rápida, la replicación de ECR copia las imágenes nuevas y las plantillas de creación de repositorios aplican la configuración, los Multi-Region Access Points de S3 dan un punto de conexión global, y el reenvío de escrituras de Aurora deja escribir desde Regiones secundarias.
- En Lambda, la simultaneidad aprovisionada preinicializa entornos en un alias o versión y se programa con Application Auto Scaling; la reservada solo reserva y limita, y en SQS la simultaneidad máxima se fija por origen de eventos. API Gateway limita por cliente con planes de uso y claves de API y reduce llamadas con la caché de etapa. ECS en Fargate puede escalar por trabajo pendiente por tarea con metric math.

Implement automated recovery processes to meet RTO and RPO requirements

- Las pruebas de conmutación se automatizan con AWS FIS (reboot-db-instances con forceFailover para RDS Multi-AZ, failover-db-cluster para clústeres) y condiciones de parada sobre alarmas. En Aurora Global Database, la transición (switchover) sirve para simulacros con RPO 0. CloudFront solo conmuta de origen con GET, HEAD y OPTIONS, y los controles de enrutamiento de ARC cambian de Región sin editar el DNS.
- AWS Backup copia puntos de recuperación a otras Regiones y cuentas con reglas de copia; las políticas de copia de Organizations aplican planes inmutables a OU enteras, y las copias entre cuentas exigen claves administradas por el cliente compartidas. Las pruebas de restauración demuestran que se puede restaurar. En S3, Replication Time Control da un tiempo de replicación con SLA y Batch Replication copia los objetos existentes.
- El ALB solo envía tráfico a destinos sanos según la comprobación del grupo de destino y, si todos fallan, abre a todos (fail open). Auto Scaling reemplaza instancias por fallos de ELB solo si se activan esas comprobaciones, con un periodo de gracia adecuado. Los umbrales de estado del grupo de destino activan la conmutación DNS con Route 53, y Automatic Target Weights aparta tráfico de destinos con errores 5xx.

4. Monitoring and Logging

15–15%

Configure the collection, aggregation, and storage of logs and metrics

- CloudWatch Logs cifra siempre los datos y admite claves de KMS simétricas por grupo de registros, cuya política usa el ARN del grupo como contexto de cifrado. Las políticas de protección de datos enmascaran datos confidenciales en la ingesta y solo logs:Unmask los muestra. En S3, Object Lock en modo de conformidad impide borrar incluso al usuario raíz, y CloudTrail valida la integridad con archivos de resumen firmados.
- Un filtro de métricas convierte los eventos que coinciden con un patrón en una métrica de CloudWatch con un valor fijo o extraído del registro, y puede añadir dimensiones de baja cardinalidad tomadas de campos JSON o delimitados. No procesa eventos anteriores a su creación, el valor predeterminado evita métricas con huecos y no se admite con dimensiones. Solo funciona en grupos de la clase Standard.
- Un flujo de métricas envía de forma continua métricas de CloudWatch a Amazon Data Firehose (y de ahí a S3, a un lago de datos o a socios externos) en formato JSON u OpenTelemetry. El flujo de Firehose debe estar en la misma cuenta y Región; los filtros son de inclusión o de exclusión, nunca ambos, y las estadísticas adicionales como p99 se configuran por métrica. En una cuenta de monitorización puede incluir las cuentas de origen.
- El agente de CloudWatch recoge métricas internas como memoria y disco, procesos con procstat y métricas de aplicación con StatsD o collectd; se instala y configura con Systems Manager usando una configuración guardada en Parameter Store, y aggregation_dimensions agrega por grupo de Auto Scaling. En Lambda, el formato de métricas integradas publica métricas desde los registros sin PutMetricData ni recopilador.
- CloudWatch Logs conserva los registros indefinidamente salvo que se fije una retención por grupo o una política de retención a nivel de cuenta, que se aplica por prefijo y puede ser retroactiva. Para archivar de forma continua se usan suscripciones a Firehose hacia S3, con reglas de S3 Lifecycle que pasan a clases Glacier y hacen caducar los objetos; en buckets con versiones hace falta NoncurrentVersionExpiration.

Audit, monitor, and analyze logs and metrics to detect issues

- Los paneles de CloudWatch pueden combinar datos de varias cuentas mediante la observabilidad entre cuentas, con una cuenta de monitorización vinculada a la organización, y se pueden compartir con personas sin cuenta de AWS mediante correo, enlace público o SSO con SAML y Amazon Cognito. AWS Quick Sight visualiza datos de Athena si se autorizan los buckets y la clave KMS, y SPICE admite actualizaciones incrementales.
- Una alarma de métrica vigila una métrica estándar o personalizada, o el resultado de una expresión matemática, y ejecuta acciones de SNS, EC2 o Auto Scaling al cambiar de estado. En métricas personalizadas la alarma debe incluir todas las dimensiones. Las métricas de alta resolución admiten alarmas de 10 o 30 segundos, y las alarmas compuestas reducen el ruido pero no ejecutan acciones de EC2 ni Auto Scaling.
- X-Ray se activa con el rastreo activo de Lambda (con AWSXRayDaemonWriteAccess en el rol de ejecución), el rastreo de las etapas de las API REST de API Gateway y, en contenedores de ECS, un sidecar de AWS Distro for OpenTelemetry con un rol de tarea. El muestreo lo decide el primer servicio rastreado, y los grupos con expresiones de filtro publican métricas en CloudWatch.
- Los filtros de suscripción de CloudWatch Logs envían eventos casi en tiempo real a Kinesis Data Streams, también entre cuentas mediante un destino con política de acceso. Para evitar limitaciones conviene la distribución Random. Los consumidores Lambda escalan con ParallelizationFactor o distribución ramificada mejorada, y Amazon Managed Service for Apache Flink calcula agregados continuos sin gestionar servidores.
- CloudWatch Logs Insights consulta de forma interactiva los registros existentes de varios grupos, con comandos como filter, stats, pattern y diff. Athena consulta con SQL los registros que los servicios dejan en S3, como CloudTrail, ALB o VPC Flow Logs, y la proyección de particiones evita gestionar particiones a mano. Los filtros de métricas no son retroactivos.

Automate monitoring and event management of complex environments

- DynamoDB escala la capacidad aprovisionada con Application Auto Scaling y seguimiento de destino, con una política propia para cada índice secundario global. RDS amplía el almacenamiento solo hasta un umbral máximo. En ECS, Service Auto Scaling ajusta las tareas y un proveedor de capacidad con escalado administrado ajusta las instancias según targetCapacity; un valor inferior al 100 % deja capacidad libre.
- Los filtros de métricas convierten eventos de CloudWatch Logs en métricas numéricas con patrones que distinguen mayúsculas y minúsculas; no son retroactivos y el valor predeterminado no se admite con dimensiones. Una alarma sobre la métrica avisa a un tema de SNS. El formato de métricas integradas permite publicar métricas personalizadas desde Lambda escribiendo registros estructurados.
- Las notificaciones de eventos de S3 entregan eventos a Lambda, SQS estándar, SNS o EventBridge; las colas FIFO solo se alcanzan mediante EventBridge. La función Lambda necesita una política basada en recursos que permita a S3 invocarla, y escribir en el mismo bucket que la activa crea un bucle. OpenSearch Ingestion indexa archivos nuevos de S3 casi en tiempo real leyendo una cola de SQS.
- Una regla de EventBridge envía a destinos como SNS los eventos que coinciden con su patrón, cuyos valores van en matrices y admiten operadores como prefix, wildcard o anything-but. Los eventos de CloudTrail requieren un registro de seguimiento activo, llegan solo al bus predeterminado y los de solo lectura necesitan el estado ENABLED_WITH_ALL_CLOUDTRAIL_MANAGEMENT_EVENTS. Los transformadores de entrada dan formato al mensaje.
- SSM Agent convierte las instancias EC2 en nodos administrados mediante un perfil de instancia o Default Host Management Configuration, que exige IMDSv2; los servidores locales se registran con una activación híbrida. El agente de CloudWatch se instala con AWS-ConfigureAWSPackage o con Quick Setup en toda la organización, necesita CloudWatchAgentServerPolicy y, sin Internet, puntos de enlace de interfaz.

5. Incident and Event Response

14–14%

Manage event sources to process, notify, and take action in response to events

- AWS Health, CloudTrail y servicios como ECS envían eventos a EventBridge, donde las reglas filtran por patrón y los envían a SNS, Lambda o Automation. Los eventos globales de Health se reciben en Norte de Virginia; los eventos de datos exigen configurarlos en el trail, y los de solo lectura, el estado ENABLED_WITH_ALL_CLOUDTRAIL_MANAGEMENT_EVENTS. Entre cuentas se necesita política en el bus receptor.
- Los flujos de eventos combinan SQS, SNS, Kinesis, Lambda y Step Functions. Con SQS, ReportBatchItemFailures evita reprocesar lo correcto y las colas de mensajes fallidos con redrive apartan y recuperan mensajes; con Kinesis, la bisección y un destino en caso de error aíslan registros erróneos. SNS con políticas de filtro distribuye a varias colas o Step Functions. Standard admite ráfagas altas.

Implement configuration changes in response to events

- Los cambios de configuración se aplican con Run Command (con control de simultaneidad y de errores), asociaciones de State Manager programadas, también en servidores locales con activación híbrida, y Automation en varias cuentas y Regiones desde un administrador delegado. AWS AppConfig valida antes de desplegar y despliega de forma gradual con reversión automática si salta una alarma.
- Los eventos pueden cambiar la infraestructura sin intervención: una alarma o un cambio en Parameter Store dispara reglas de EventBridge que ejecutan runbooks como AWS-ResizeInstance o actualizan plantillas de lanzamiento; la actualización de instancias con reversión automática exige versiones numeradas. Los enlaces del ciclo de vida de Auto Scaling, el disyuntor de ECS y EventBridge Scheduler completan el repertorio.
- Para devolver un sistema a su estado deseado se combinan asociaciones de State Manager que reaplican la configuración, reglas de EventBridge que ejecutan runbooks de Automation (por ejemplo, para aislar instancias o reactivar CloudTrail), OpsItems de OpsCenter con runbooks asociados, comprobaciones de estado personalizadas de Auto Scaling y manejo de errores con Retry y Catch en Step Functions.

Troubleshoot system and application failures

- En CodeDeploy, los scripts de ApplicationStop salen de la última revisión correcta y un error 'Missing credentials' del agente apunta al perfil de instancia. Una pila en UPDATE_ROLLBACK_FAILED no se actualiza: se corrige la causa (por ejemplo, con signal-resource) y se continúa la reversión. CodeBuild y CodePipeline fallan por permisos del rol de servicio, y un canario en una VPC sin Internet necesita puntos de enlace para CloudWatch y S3.
- El historial de actividad de Auto Scaling explica los lanzamientos fallidos y las terminaciones; un periodo de gracia más corto que el arranque provoca bucles de sustitución. En ECS, los eventos del servicio, minimumHealthyPercent y maximumPercent y el disyuntor con reversión explican los despliegues atascados, y Fargate en subredes privadas necesita puntos de enlace de ECR y S3. En EKS, HPA necesita Metrics Server.

6. Security and Compliance

17–17%

Implement techniques for identity and access management at scale

- IAM Access Analyzer genera políticas a partir de la actividad de CloudTrail, aunque no incluye iam:PassRole ni las acciones de eventos de datos; sus comprobaciones personalizadas detectan acceso nuevo en una canalización y los analizadores de acceso no utilizado señalan roles y permisos sin uso en toda la organización. Los límites de permisos fijan el máximo de los roles delegados, y el último acceso de una OU ayuda a ajustar sus SCP.
- RBAC asigna políticas por función laboral, como los conjuntos de permisos de IAM Identity Center que se convierten en roles en cada cuenta. ABAC compara etiquetas de la entidad principal y del recurso (aws:PrincipalTag, aws:ResourceTag, aws:RequestTag) y escala sin tocar políticas; los atributos del IdP llegan como etiquetas de sesión, que exigen sts:TagSession en la política de confianza.
- Secrets Manager rota secretos con rotación administrada (por ejemplo, la contraseña maestra de RDS o Aurora con ManageMasterUserPassword) o con una función Lambda; la estrategia de usuarios alternos mantiene credenciales válidas durante la rotación. Una función en una VPC sin Internet necesita un punto de enlace de Secrets Manager.
- La MFA para la API se exige con aws:MultiFactorAuthPresent, en la política de confianza del rol para el acceso entre cuentas y con BoolIfExists para denegar también las claves de larga duración, el usuario pasa el dispositivo y el código a AssumeRole o GetSessionToken. Las identidades de máquina usan credenciales temporales: perfiles de instancia en EC2, roles de tarea en ECS y EKS Pod Identity en Kubernetes.

Apply automation for security controls and data protection

- La configuración central de Security Hub CSPM aplica estándares y controles en cuentas y Regiones y evita desviaciones; sus reglas de automatización actualizan hallazgos al recibirlos. Control Tower tiene controles preventivos (SCP), detectivos (reglas de Config) y proactivos (hooks de CloudFormation). Los paquetes de conformidad de la organización se despliegan por Región, y Automation multicuenta usa roles de administración y de ejecución.
- La defensa en profundidad combina capas: grupos de seguridad con estado y solo reglas de permiso, ACL de red sin estado con denegaciones por subred, AWS WAF en ALB, CloudFront o API Gateway con reglas basadas en tasa y grupos administrados, y Network Firewall en el perímetro de la VPC con filtrado por dominio. GuardDuty detecta, EventBridge automatiza la respuesta, Detective investiga y ACM renueva solo los certificados que emite.
- Amazon Macie automatiza el descubrimiento de datos confidenciales en S3 de dos formas: la detección automatizada, que muestrea objetos de forma continua en toda la organización desde un administrador delegado, y los trabajos de detección, periódicos o puntuales, con criterios de bucket que se evalúan en cada ejecución. Los identificadores personalizados y las listas de permitidos afinan qué se detecta y qué se ignora.
- Para el cifrado en tránsito, ACM renueva automáticamente los certificados emitidos por Amazon con validación por DNS (no los importados) y la condición aws:SecureTransport en la política del bucket rechaza las solicitudes HTTP. En reposo, KMS rota el material de claves sin cambiar la clave lógica, un almacén de claves de CloudHSM aporta HSM de un solo inquilino y compartir instantáneas cifradas exige una clave administrada por el cliente.

Implement security monitoring and auditing solutions

- Una auditoría robusta parte de un trail de la organización, que cubre todas las cuentas y no pueden modificar los miembros, con validación de integridad mediante archivos de resumen firmados y S3 Object Lock en modo de cumplimiento para conservar los registros en WORM. AWS Config despliega paquetes de conformidad para toda la organización desde un administrador delegado, e IAM Access Analyzer detecta accesos no utilizados.
- Las alertas de seguridad combinan CloudTrail Insights, que detecta desviaciones de la tasa normal de llamadas o errores de API, con reglas de EventBridge sobre eventos de CloudTrail y hallazgos de GuardDuty, que admiten coincidencia numérica y deben habilitarse para eventos de solo lectura si se necesitan. Para umbrales por recuento se usan filtros de métricas con alarmas, y un bus central recibe eventos de toda la organización.
- CloudTrail registra eventos de administración y, solo si se configuran con selectores avanzados, eventos de datos como las operaciones de objetos de S3. En CloudWatch Logs, los destinos y las políticas de suscripción de nivel de cuenta centralizan registros casi en tiempo real, una clave de KMS simétrica asociada al grupo cifra los datos y las políticas de protección de datos enmascaran información confidencial al ingerirla.
- Athena con proyección de particiones consulta los registros de CloudTrail en S3 sin mantener particiones, y Logs Insights consulta grupos de registros de cualquier periodo pasado; los filtros de métricas no son retroactivos. Detective investiga hallazgos de GuardDuty con gráficos de comportamiento, AWS Security Hub los correlaciona en hallazgos de exposición y las consultas avanzadas de Config con agregador abarcan la organización.