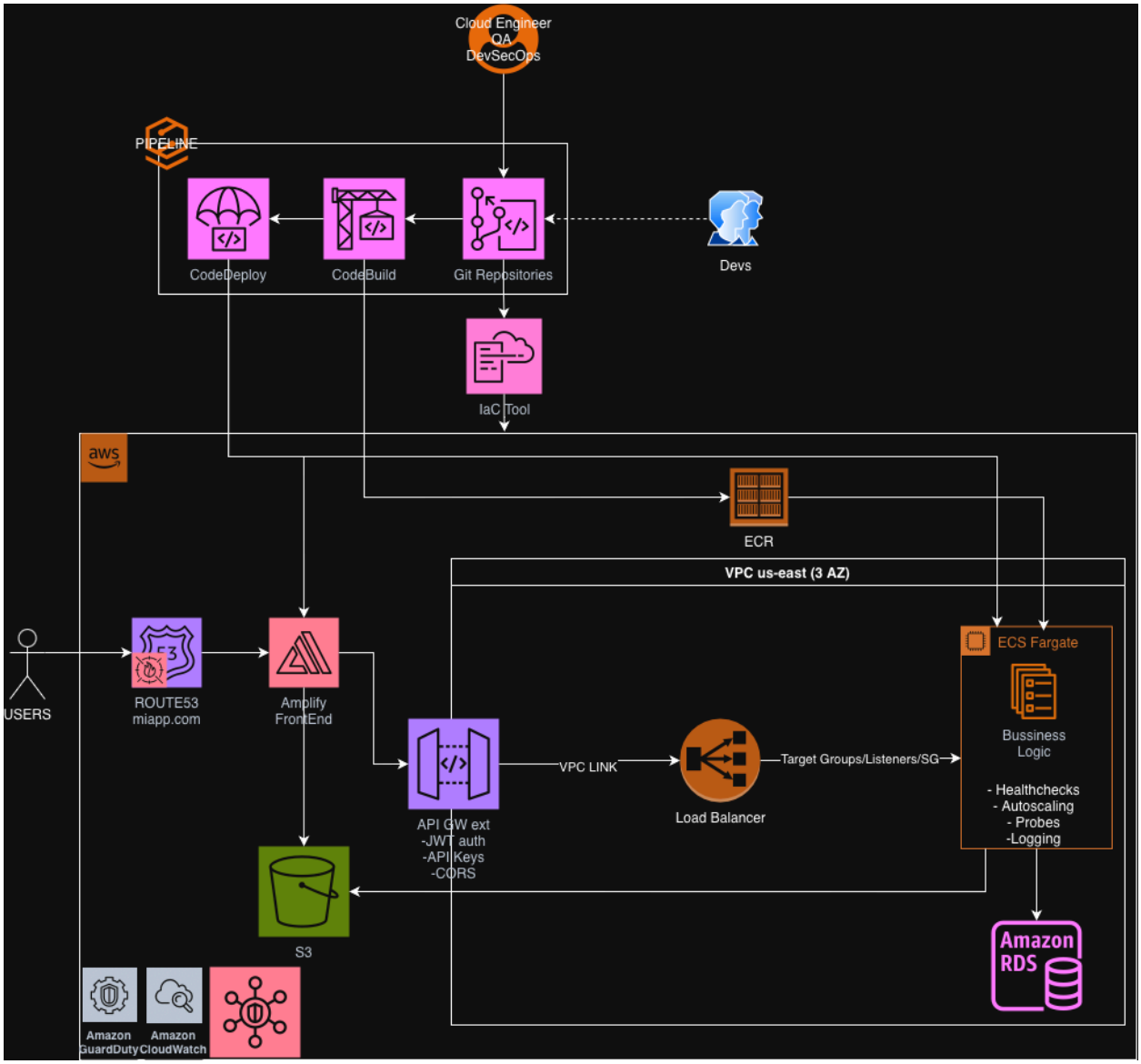
1. La nube pública es un servicio al que se puede acceder mediante internet, la nube privada es un servicio al que solo se puede acceder desde una red corporativa y la nube híbrida tiene parte de sus servicios accesibles mediante internet y otros son estrictamente a través de una red privada, esto se logra mayormente mediante el uso de túneles VPN o servicios de enrutamiento con proveedores que tienen enlaces dedicados.
2. Tres prácticas de seguridad en la nube son:
    a. No root login solo para breakglass
    b. No usuarios IAM usar idP federado
    c. MFA obligatorio
3. Infraestructura como código o IaC te permite replicar distintos ambientes y autorizar tus despliegues usando código en lugar de ir dándole click uno a uno a tu proyecto, esto reduce enormemente el error humano y mantienen consistencia en tus recursos creados como nombres, tags y otros. Dos herramientas populares son Terrform y Ansible, aunque puedes encontrar herramientas propias de los proveedores de nube como cloudformation de AWS y bicep en azure.
4. Las métricas más útiles en la nube son TPS(transacciones por segundo) y usuarios concurrentes aunque dependiendo del servicio puedes evaluar uso de recursos como memoria y CPU para evaluar si requieres aplicar reglas de autoescalamiento.
5. Docker es un motor de contenedores, es básicamente un software que permite gestionar contenedores. Sus principales componentes son: Engine, Imagenes, Contenedores, Dockerfile, entre otros.

6. 

La solución implementa una arquitectura moderna en AWS basada en desacoplamiento entre frontend, orquestación de API y microservicios en contenedores.
El flujo comienza con los desarrolladores, quienes gestionan el código en Git Repositories y disparan un pipeline CI/CD a través de CodeBuild y CodeDeploy para desplegar los cambios en los servicios, también se automatiza el despliegue de la infraestructura mediante un IaC Tool que provisiona todos los recursos necesarios en AWS.

El frontend se despliega en AWS Amplify Hosting, quedando accesible mediante un dominio administrado en Route53. Los usuarios consumen la aplicación web y esta realiza llamadas seguras hacia un API Gateway externo, el cual aplica controles de seguridad como WAF, autenticación, API Keys y políticas CORS.

API Gateway enruta el tráfico interno hacia los microservicios mediante un VPC Link, que conecta directamente con un Load Balancer privado dentro de la VPC. Este balanceador distribuye las solicitudes hacia tareas ECS Fargate, donde reside la lógica de negocio contenida en imágenes almacenadas previamente en ECR.

Cada servicio en Fargate está configurado con autoescalamiento, health checks, registros centralizados y mediante Security Groups reforzamos que el tráfico se dirija solo en los puertos asignados y evitamos brechas de seguridad. Las aplicaciones se integran finalmente con Amazon RDS para el manejo persistente de datos.

Todo el entorno está protegido y monitoreado con herramientas nativas como CloudWatch, GuardDuty y servicios de networking aislado en una VPC distribuida en 3 Availability Zones, garantizando alta disponibilidad, seguridad y escalabilidad.

Aunque no se ha agregado los actores que tienen acceso a los ambientes en AWS, es importante mencionar que estos roles se administran desde un proveedor de identidad federado, lo que evita tener usuarios IAM, el acceso root no esta permitido excepto para ciertos casos muy específicos, MFA activado y para asegurarnos que todos los recursos cumplan con los requerimientos de forma y seguridad se aplica Config y SCPs