DISEÑO DE ARQUITECTURA PRODUCCIÓN EN AMAZON WEB SERVICES

Proyecto: Banca Móvil

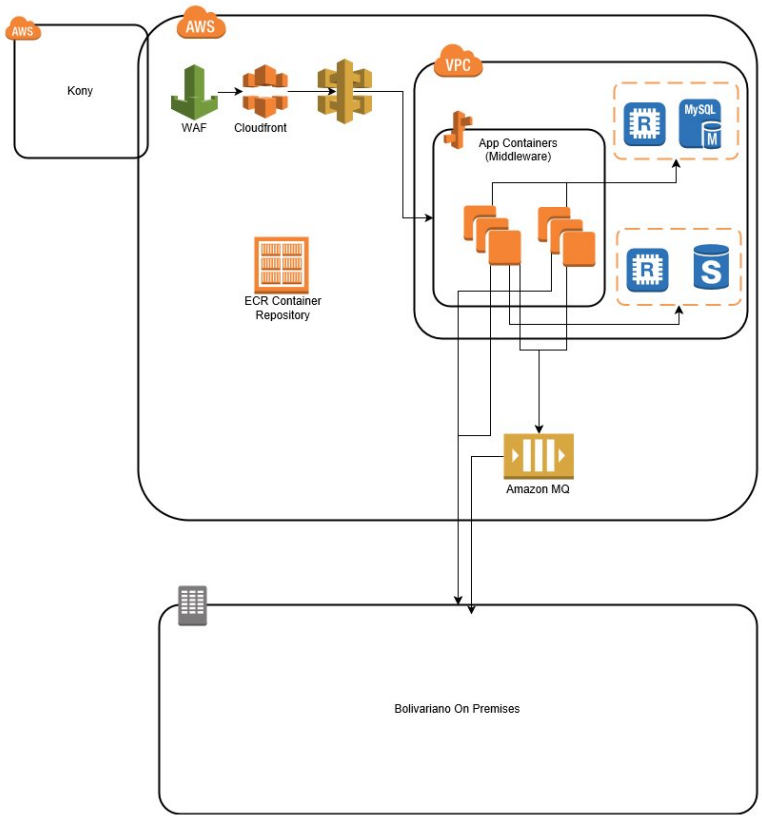
Francisco Fagas
Francisco.Fagas@softwareone.com
Solutions Specialist
SoftwareOne Ecuador

Version 1.0, Fecha: 23 de Abril de 2018

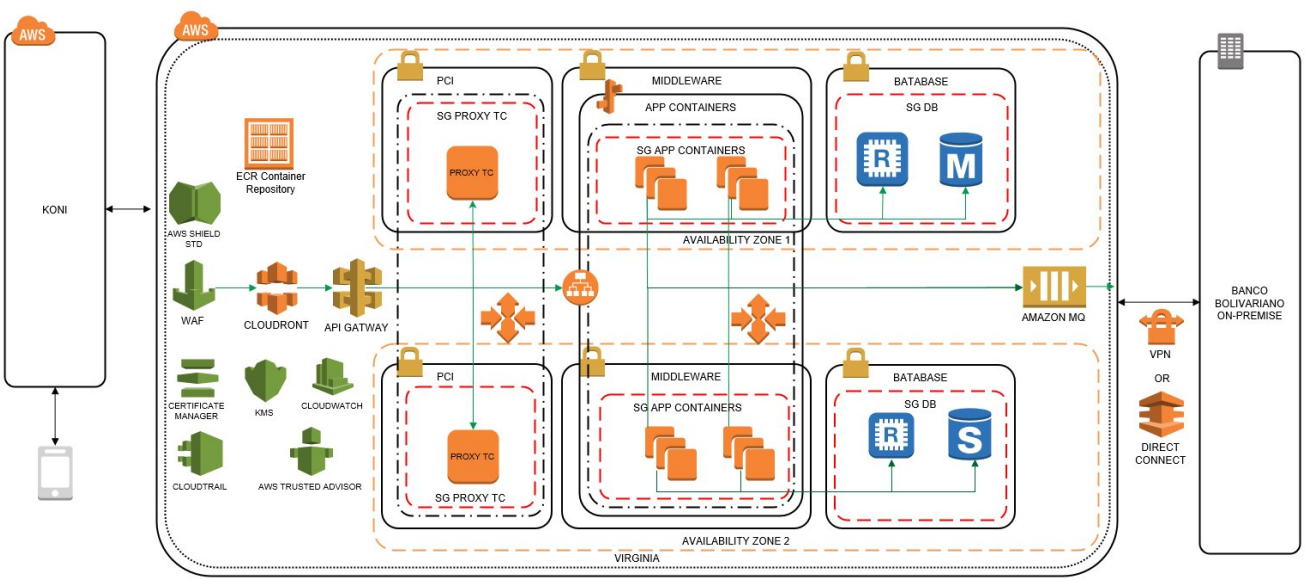
AMBIENTE DE PRODUCCIÓN

Diagramas de Arquitectura

High Level View



Detailed View



Definición de Componentes

Componente AWS	Descripción
1. Virtual Private Cloud (VPC)	Aprovisionamiento de Amazon en la VPC aisladas de forma lógica.
2. Subnet	Segmentos dentro de una VPC, conectadas a través de la tabla de ruteo. Cada segmento tiene su ACL para la autorización o denegación de conexiones de entrada y salida. Ninguna de las subnets están conectadas a internet.
3. Security Groups	Firewall virtual que controlará el trafico a la instancia EC2 y RDS. Se asocia un grupo de seguridad por recurso y se establecerá las reglas de tráfico a cada uno de ellos según lo especificado por el proveedor. El proveedor deberá especificar los puertos y protocolos para las reglas de cada grupo de seguridad.
4. Elastics Beanstalk	Servicio para implementar servicios y aplicaciones web en Java, .Net, PHP, Node.js, Python, Ruby, Go y Docker en servicios como apache, Ngnix, Passenger e IIS. Las instrucciones se ejecutan sobre instancias EC2 lo cual permite conectarse a la instancia en caso se requiera instalar componentes adicionales. Detalle de plataformas admitidas: https://docs.aws.amazon.com/es_es/elasticbeanstalk/latest/dg/concepts.platforms.html
5. EC2 Instance	Servicio web de capacidad informática de tamaño modificable
6. Elastics Block Storage (EBS)	En EBS se provisionarán los volúmenes de almacenamiento en bloques persistentes utilizado por las instancias EC2. Se recomienda desacoplar el almacenamiento de logs y recursos de los volúmenes de EBS para cuando auto-scalling está habilitado.
7. Bucket de S3	El servicio de Amazon S3 cumple 3 funciones en la arquitectura planteada: 1. Almacenamiento de los snapshots de los volúmenes de EBS. 2. Repositorio de código y cambios de Beanstalk. 3. Almacenamiento de logs.
8. Relational Database Service (RDS)	Servicio administrado de base de datos de Amazon. Soporte de MySQL desde las versiones 5.5 a 5.7. Configurado con alta disponibilidad en multi AZ. https://docs.aws.amazon.com/es_es/AmazonRDS/latest/UserGuide/CHAP_MySQL.html#MySQL.Concepts.VersionMgmt
9. AWS Config	Con AWS Config Banco Bolivariano examinará, auditará y evaluará las configuraciones de los recursos de AWS para los ambientes de desarrollo y QAS.

Definición de Componentes

Componente AWS	Descripción
10. Elastics Cache - Redis	Amazon ElastiCache para Redis funcionará como almacén de datos en memoria para brindar tiempos de respuesta inferiores a un milisegundo. A diferencia de las bases de datos basadas en discos, en las que la mayoría de las operaciones necesitan ir y volver al disco, los almacenes de datos en memoria administran los datos en memoria, que es mucho más rápido que hacerlo en discos. El resultado es un mayor desempeño en operaciones de lectura o escritura promedio que se ejecutan en menos de un milisegundo y capacidad para procesar millones de operaciones por segundo.
11. Amazon MQ	Servicio de agente de mensajes administrado para Apache ActiveMQ que facilita la configuración y operación de agentes de mensajes en la nube. Los agentes de mensajes permiten que diferentes contenedores o sistemas de software se comuniquen e intercambien información. Amazon MQ gestiona la administración y el mantenimiento de ActiveMQ, la infraestructura subyacente está provisionada automáticamente para una alta disponibilidad y la durabilidad de los mensajes con el fin de dar soporte a la fiabilidad de sus aplicaciones. Protocolos estándar del sector soportados para mensajerí: JMS, NMS, AMQP, STOMP, MQTT y WebSocket. *Amazon MQ dentro de la arquitetura planteada no es el único componente de integración con los sistemas del banco, la llamada directa desde la capa de middleware a componentes on-Premise es posible realizar a través de la VPN o Direct Connect.
12. ECR Container Registry	Amazon Elastic Container Registry (ECR) es un registro de contenedores de Docker completamente administrado que les facilitará las tareas de almacenamiento, administración e implementación de imágenes de contenedores de Docker. Amazon ECR se integra con Amazon Elastic Container Service (ECS), lo que permite simplificar el desarrollo para el flujo de trabajo de producción. Con Amazon ECR, ya no es necesario que utilice sus propios repositorios de contenedores ni se preocupe por tener que escalar la infraestructura subyacente. Amazon ECR hospeda sus imágenes en una arquitectura escalable y de alta disponibilidad, lo que le permite implementar contenedores para sus aplicaciones con fiabilidad. La integración con AWS Identity and Access Management (IAM) ofrece un control de cada repositorio a nivel de recurso.
13. Amazon API Gateway	Amazon API Gateway es un servicio completamente administrado que facilitará la creación, la publicación, el mantenimiento, la monitorización y la protección de las API a cualquier escala. Con tan solo unos clics en la consola de administración de AWS, puede crear una API que haga las veces de "puerta delantera" para que las aplicaciones obtengan acceso a datos, lógica de negocio o funcionalidades desde sus servicios de backend, como cargas de trabajo ejecutadas en Amazon Elastic Compute Cloud (Amazon EC2), código ejecutado en AWS Lambda o cualquier aplicación web.
14. CloudFront	Amazon CloudFront es un servicio de red de entrega de contenido (CDN) global que proporciona datos, vídeos, aplicaciones y API de forma segura a sus espectadores con baja latencia y altas velocidades de transferencia. CloudFront se integra con AWS, incluidas las ubicaciones físicas conectadas directamente a la infraestructura global de AWS, como con el software que funciona a la perfección con los servicios que incluyen AWS Shield para la mitigación de ataques DDoS, Amazon S3, Elastic Load Balancing o Amazon EC2, como orígenes de sus aplicaciones, y Lambda@Edge para ejecutar código personalizado cerca de sus espectadores.

Definición de Componentes

Componente AWS	Descripción
15. Servicios de Seguridad	3.1. AWS Shield Standard ofrece protección ante los ataques DDoS más comunes, que normalmente ocurren en la capa de red y transporte, y que están dirigidos a su aplicación o sitio web. Cuando usa AWS Shield Standard con Amazon CloudFront y Amazon Route 53, recibe protección de disponibilidad integral contra todos los ataques a infraestructura (capa 3 y 4) conocidos. 3.2. AWS WAF es un firewall web que ayudará a proteger la aplicación web de ataques web habituales que podrían afectar a la disponibilidad de la aplicación, comprometer la seguridad o consumir excesivos recursos. AWS WAF permite controlar el tráfico que desea habilitar o bloquear en su aplicación web mediante la definición de reglas de seguridad web personalizables. 3.3 Amazon Cloud Watch visualizar el monitoreo detallado de las instancias EC2. 3.4. Con AWS Certificate Manager se solicitará rápidamente el certificado, implementarlo en el balanceador de Elastic Load Balancer, Certificate Manager se ocupará de renovar los certificados. 3.5. Con Cloud Trail le permitirá a seguridad informática realizar regulaciones y auditorías operativas, de riesgo y conformidad. 3.6. Con el servicio administrado de AWS Key Management Service (KMS) se creará y controlará las claves de cifrado que se utilizará para cifrar los datos. 3.7. Con AWS Config Banco Bolivariano examinará, auditará y evaluará las configuraciones de los recursos de AWS del ambiente de producción.

Revisión y Aceptación:	**Entrega:**
Nombre: Miguel Salazar **Cargo:** Arquitectura **Empresa:** Banco Bolivariano	**Nombre:** Francisco Fagas **Cargo:** Solutions Sales **Empresa:** SoftwareOne Ecuador Soluciones