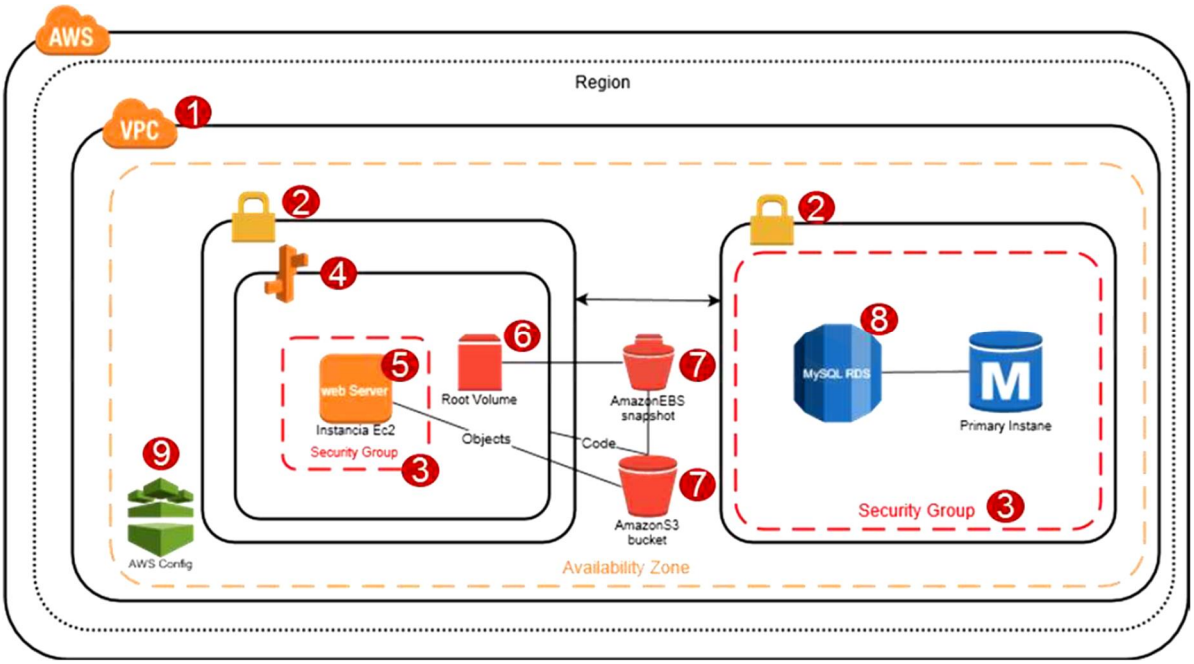
DISEÑO DE ARQUITECTURA BOLIVARIANO.COM

El presente documento describe la arquitectura que se utilizará para la implementación de la solución bolivariano.com en la nube de Amazon (AWS).

DIAGRAMA DE ARQUITECTURA

AMBIENTE DE DESARROLLO



COMPONENTES DE AWS

1. Virtual Private Cloud (VPC)
Aprovisionamiento de Amazon VPC para desarrollo y QAS aisladas de forma lógica.

2. Subnet
Segmentos dentro de cada una de las VPCs de desarrollo y QAS, 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 tráfico 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. Soporte de IIS desde 7.5. 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. Instancia de 2 cores y 4 GB de ram para los ambientes de desarrollo y QAS con sistema operativo Windows.

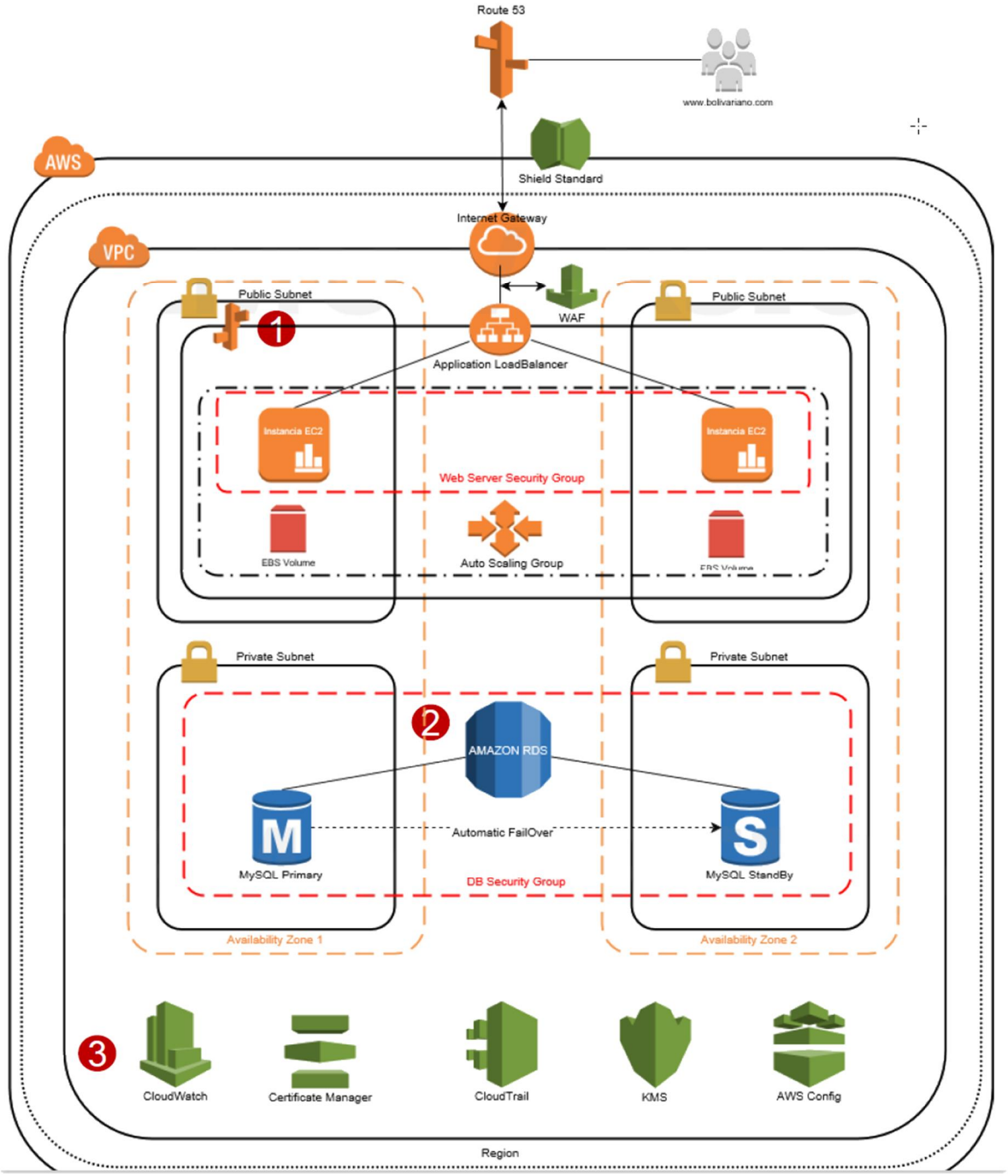
6. Elastics Block Storage (EBS)
En EBS se provisionarán los volúmenes de almacenamiento en bloques persistentes utilizado por las instancias EC2 de desarrollo y QAS. 110 GBs por servidor web por ambiente distribuidos 10 GB para sistema operativo y 100 GB disponibles en discos magnéticos. Se recomienda 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 los objetos como imágenes, videos, logs otro tipo de archivo que pueda utilizar el sitio bolivariano.com.

8. Relational Database Service (RDS)
Servicio administrado de base de datos de Amazon. Soporte de MySQL desde las versiones 5.5 a 5.7. Para los ambientes de desarrollo y QAS se realizará sin alta disponibilidad en una única zona de disponibilidad.
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.

AMBIENTE DE PRODUCCIÓN



COMPONENTES DE AWS

1. Elastics Beanstalk

Para el ambiente de producción Beanstalk se configura dos instancias con monitoreo detallado Windows de 4 cores y 16 GB de ram en modo activo-activo, configuración de auto scaling y con balanceo utilizando Application Load balancer, configuraciones de reglas WAF y tráfico encriptado con Certificate Manager.

Tal como se mencionó en desarrollo los volúmenes de EBS deben estar desacoplados de data como logs, imágenes, videos y cualquier otro recurso que deba ser movido a buckets de S3. Los volúmenes EBS y snapshots se encontrarán encriptados.

2. Relational Database Service (RDS)

El servicio de RDS con MySQL estará configurado en multi zona de disponibilidad con failover automático. Los datos de de RDS también se encontrarán encriptados.

3. Servicios de Seguridad

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.

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.

Amazon Cloud Watch visualizar el monitoreo detallado de las instancias EC2.
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.

Con Cloud Trail le permitirá a seguridad informática realizar regulaciones y auditorías operativas, de riesgo y conformidad.

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.

Con AWS Config Banco Bolivariano examinará, auditará y evaluará las configuraciones de los recursos de AWS del ambiente de producción.

De no existir observaciones se concluye que las partes tienen pleno conocimiento de los elementos definidos para la arquitectura, del alcance, de la funcionalidad, de la compatibilidad con la solución adquirida y se acepta la infraestructura sobre la cual será implementado el portal para bolivariano.com.

Revisión y Aceptación:

Juan Gaibor **Gerente Infraestructura**	Miguel Salazar **Gerente Arquitectura**	I-Route