Arquitectura de Soluciones:

Informe de la arquitectura propuesta para el Banco BP

Tabla de índices.

Introducción

El presente documento técnico de arquitectura de soluciones tiene como objetivo detallar los componentes necesarios para el diseño e implementación de la arquitectura de solución. Este informe presenta las posibles soluciones, patrones de arquitectura y patrones SOA para garantizar una arquitectura robusta, escalable y de alta calidad. La arquitectura planteada se basa en un enfoque centrado en el cliente, que busca garantizar una experiencia óptima para los usuarios finales del aplicativo. En este informe se describen las diferentes capas y componentes del sistema, así como su interacción y dependencias, con el fin de brindar una visión completa de la arquitectura propuesta.

Antecedentes

Se requiere diseñar un sistema de banca por internet que permita a los usuarios acceder al histórico de sus movimientos, realizar transferencias y pagos entre cuentas propias e interbancarias. La información del cliente se tomará de dos sistemas: una plataforma Core que contiene información básica de cliente, movimientos y productos; y un sistema independiente que complementa la información del cliente cuando se requieren datos detallados. El sistema debe notificar a los usuarios sobre los movimientos realizados, utilizando al menos dos sistemas externos o propios de envío de notificaciones. El sistema consta de dos aplicaciones front-end: una SPA y una aplicación móvil desarrollada en un framework multiplataforma.

Ambas aplicaciones autentican a los usuarios mediante un servicio que utiliza el estándar OAuth 2.0, para el cual se cuenta con un producto que puede ser configurado para este fin. El sistema de Onboarding para nuevos clientes en la aplicación móvil utiliza reconocimiento facial como parte del flujo de autorización y autenticación. A partir del Onboarding, el nuevo usuario puede ingresar al sistema mediante usuario y clave, huella o algún otro método especificado dentro de la arquitectura. El sistema utiliza una base de datos de auditoría que registra todas las acciones del cliente y cuenta con un mecanismo de persistencia de información para clientes frecuentes.

Para obtener los datos del cliente, el sistema pasa por una capa de integración compuesta por un API Gateway y consume los servicios necesarios de acuerdo con el tipo de transacción. Inicialmente, se cuenta con tres servicios principales: consulta de datos básicos, consulta de movimientos y transferencias que realizan llamados a servicios externos dependiendo del tipo.

Diseño del modelo de la arquitectura

Características técnicas

Para poder cumplir con los requisitos solicitados por el Banco Digital BP y para garantizar una correcta arquitectura enfocada a la nube para el manejo correcto de los costos y escalabilidad que cumplan con los estándares solicitados se ha propuesto el siguiente diseño de arquitectura:

1. Elementos normativos

Para esto, la arquitectura va usar las siguientes normas para cumplir con las leyes o regulaciones:

- Leyes de protección de datos personales:
  Es importante cumplir con las leyes y regulaciones locales e internacionales en relación a la privacidad y la protección de los datos personales de los clientes.

  Para esto se debe de revisar todos los datos que el cliente va a guardar y verificar que únicamente los datos que no son sensibles se puedan almacenar en la nube y e identificar que datos se puede enmascarar o encriptar para poder almacenar en la base de datos, colocar un correcto almacenamiento de información en Cognito de los usuarios de los clientes

- Normativas de seguridad financiera:
  Se deben cumplir las regulaciones que establecen las medidas de seguridad que deben tener los sistemas financieros para proteger a los clientes y prevenir fraudes.

  En la arquitectura propuesta se va a implementar doble autenticación y colocar todos los servicios con Ouath 2 para proteger la comunicación de los microservicios, así como colocar en privado todos los microservicios que manejen datos sensibles, manejar la información de las Apis en Secret Manager.

- Regulaciones sobre transferencias internacionales:
  Se deben cumplir las regulaciones que establecen las normas para las transferencias internacionales, incluyendo la prevención del lavado de dinero y la financiación del terrorismo.

  Se debe de crear Dashboard en Power Bi de todos los clientes que hagan transferencias internacionales para poder verificar todos los movimientos para verificar el lavado de dinero, así como controles en los movimientos del cliente.

- Normativas sobre notificaciones:
  Se deben cumplir las regulaciones que establecen la forma en que se deben notificar las transacciones a los clientes, para garantizar que estén informados de todas las transacciones realizadas en su cuenta.

  En la arquitectura propuesta va a tener un modulo para las notificaciones en diferentes canales como Push (Firebase), SMS, Email, adicional se va agregar un componente de tercero para manejar las notificaciones con Braze que es SDK de terceros que permite administrar notificaciones según los eventos que se van generando.

- Estándares de autenticación: se deben cumplir con los estándares de autenticación establecidos, para garantizar que solo los usuarios autorizados puedan acceder al sistema.

  Para esto se va a realizar un microservicio que va servir para la autenticación donde los usuarios van a estar configurados en Cognito así como en una tabla de usuarios propiamente.

2. Alta disponibilidad (HA) y tolerancia a fallos (DR) seguridad y monitoreo:

Para garantizar alta disponibilidad (HA) y tolerancia a fallos (DR) en la arquitectura del sistema de banca por internet, se pueden seguir las siguientes prácticas:

- Se va a implementar una arquitectura de múltiples zonas de disponibilidad (AZ) y regiones: esto permite que el sistema se ejecute en diferentes zonas de disponibilidad y regiones, lo que garantiza que el sistema seguirá funcionando incluso si una zona o región se cae.

- Implementar múltiples réplicas: Para garantizar la disponibilidad continua del servicio, se pueden implementar múltiples réplicas de los contenedores Docker en el clúster de EKS. Esto asegura que, si una instancia falla, las otras pueden continuar sirviendo las solicitudes.

- Utilizar almacenamiento de datos redundante y distribuido: esto garantiza que los datos estén siempre disponibles y que no se pierdan en caso de una falla del sistema.

- Realizar copias de seguridad y recuperación ante desastres: esto garantiza que se pueda recuperar el sistema en caso de una falla mayor.

En cuanto a la seguridad y el monitoreo, se pueden seguir las siguientes prácticas:

- Implementar políticas de seguridad adecuadas, como la autenticación de usuarios, la autorización, el cifrado de datos, la gestión de claves y el control de acceso.

- Realizar pruebas de penetración y pruebas de seguridad regulares para identificar posibles vulnerabilidades y corregirlas.

- Utilizar herramientas de monitoreo y análisis de logs para detectar posibles problemas de seguridad o rendimiento.

- Implementar mecanismos de alerta temprana para detectar posibles fallas o problemas de rendimiento antes de que afecten a los usuarios.

- Capacitar al personal para que siga buenas prácticas de seguridad y se mantenga actualizado sobre las nuevas amenazas y vulnerabilidades.

En general, garantizar alta disponibilidad, tolerancia a fallos, seguridad y monitoreo es esencial para la arquitectura de un sistema de banca por internet, y se deben seguir las mejores prácticas y utilizar los servicios y herramientas adecuados para lograrlo.

3. Diseñar los elementos de Infraestructura de AWS:

Para diseñar los elementos de infraestructura en la nube de AWS y garantizar baja latencia, se pueden seguir las siguientes prácticas:

- Utilizar una red privada virtual (VPC): esto permite que el sistema se ejecute en una red virtual aislada en la nube de AWS, lo que garantiza la seguridad de los datos y reduce la latencia al minimizar el tráfico en la red pública.

- Utilizar servicios de almacenamiento en caché: esto permite que los datos se almacenen en caché en la memoria de acceso aleatorio (RAM) para acelerar el acceso a los datos y reducir la latencia.

- Utilizar servicios de balanceo de carga y escalado automático: esto permite que el sistema se ajuste automáticamente en función de la demanda, lo que garantiza que el sistema estará disponible y con capacidad suficiente para procesar las solicitudes, reduciendo la latencia.

- Utilizar servicios de CDN (Content Delivery Network): esto permite que los contenidos se distribuyan a través de una red global de servidores para acelerar su acceso y reducir la latencia.

- Utilizar bases de datos y servicios que estén cerca de los usuarios: esto permite que los usuarios accedan a los datos de manera más rápida y con menos latencia.

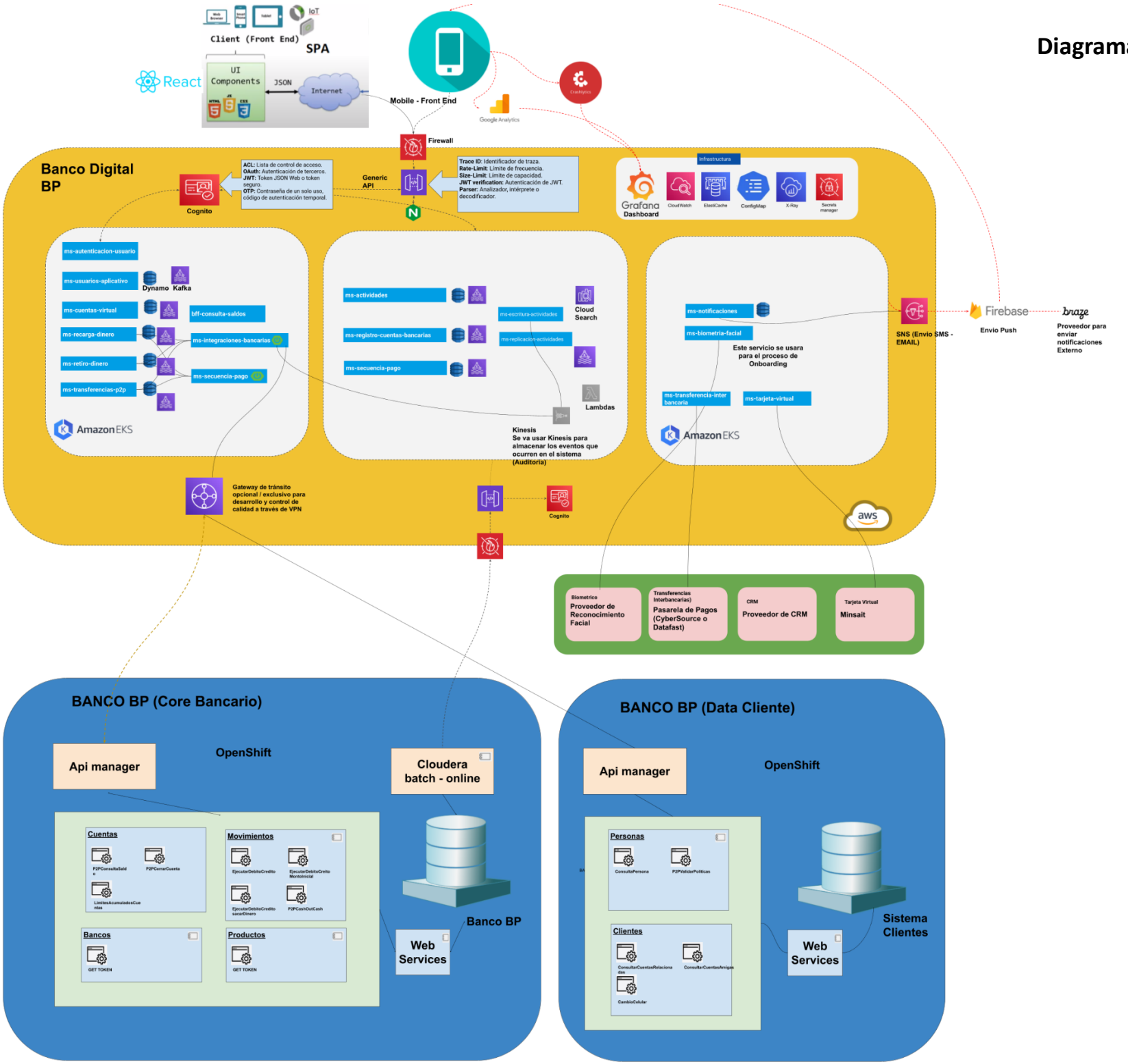
- Utilizar los servicios de AWS que ofrecen baja latencia, como AWS Direct Connect, Amazon Route 53 Latency-Based Routing, Amazon Elastic File System (EFS) y Amazon Aurora.

4. Modelo desarrollado bajo modelo c4, contenedores y componentes:

Para desarrollar el modelo de arquitectura bajo el modelo C4, se pueden seguir los siguientes pasos:

1. Identificar el contexto: describir los actores externos al sistema y los sistemas externos con los que interactúa.
2. Identificar los contenedores: identificar los componentes de nivel superior que proporcionan funcionalidad y se ejecutan en un entorno separado.
3. Identificar los componentes: descomponer los contenedores en componentes de menor nivel que implementan la funcionalidad específica.
4. Identificar las relaciones: identificar las relaciones entre los componentes y los contenedores, así como las interfaces y los protocolos que se utilizan para comunicarse.

Diagrama de Componentes



5. Explorando el corazón de nuestro sistema: El diagrama de componentes:

Aplicativos

- En la parte superior se encuentran dos aplicativos. Uno de ellos es una SPA (realizado en React), mientras que el otro es una aplicación móvil desarrollada para Android/iOS (ubicado en el front-end).

- Al utilizar React para el desarrollo del aplicativo SPA del Banco Digital, se puede lograr una gran eficiencia y productividad, ya que se puede reutilizar el código y las funcionalidades en diferentes secciones de la aplicación. También es fácil de integrar con otros componentes y tecnologías, lo que permite la construcción de una aplicación escalable y flexible.

- Front (Android/Ios)
  Estas aplicaciones se comunicarán con los servicios del Banco Digital a través del API Gateway expuesto en AWS, utilizando protocolos de comunicación estándar como HTTP o HTTPS y JSON como formato de intercambio de datos.

- Además, se implementarán funcionalidades específicas para cada plataforma, como el uso de notificaciones push para dispositivos móviles, la integración con sistemas de pago como Apple Pay o Google Pay, y la implementación de medidas de seguridad nativas como FaceID o TouchID en dispositivos de Apple.

Conexión con servicios públicos

- Los aplicativos se conectarán a los servicios públicos expuestos en AWS a través del API Gateway. Para ingresar a AWS, deberán pasar primero por el Firewall.

Configuraciones del API Gateway

- El API Gateway tendrá las siguientes configuraciones:
  - Trace ID: Identificador de traza.
  - Rate-Limit: Límite de frecuencia.
  - Size-Limit: Límite de capacidad.
  - JWT verification: Autenticación de JWT.
  - Parser: Analizador, intérprete o decodificador.

Autenticación de usuarios

- Cuando el usuario hace el Login, se invocará al servicio ms-autenticacion-usuario. Este servicio realizará primero la consulta a Cognito para verificar que el usuario que está iniciando sesión es correcto. Posteriormente, se verificará la información adicional del usuario en la tabla de Dynamo Usuario.

Dashboard

- Dentro del aplicativo se mostrará un dashboard que incluirá los movimientos de la cuenta y el saldo del cliente. Para ello se utilizará el servicio **bff-consulta-saldos** para hacer la consulta correspondiente.

Actualizaciones de movimientos y saldos

- En caso de que el cliente realice transacciones desde otro canal que no sea el aplicativo móvil, el Core del Banco enviará las actualizaciones de movimientos y saldos a través de un servicio expuesto en AWS. Este servicio tendrá credenciales específicas para su consumo y el usuario podrá recibir las actualizaciones correspondientes.

Servicios web en el Core del Banco

- Dentro del Core del Banco, se contarán con servicios web para los módulos de cuentas, movimientos y productos, los cuales estarán expuestos a través de la herramienta OpenShift. Estos servicios se comunicarán con la base de datos del core. La comunicación entre el Core del Banco y el Banco Digital se realizará de dos formas: Batch y en línea.

Comunicación con el otro sistema del banco

- Además, el otro sistema del banco contará con servicios web para los módulos de clientes, direcciones y personas. Este sistema se comunicará con el Banco Digital a través de la herramienta OpenShift, al igual que el Core de Cuentas. El proceso de comunicación se realizará en dos formas: Batch y en línea.

Registro de información proveniente de sistemas externos

- Para registrar toda la información proveniente de los sistemas externos, tanto del Core de Cuentas como del Core de Clientes, se utilizará el servicio **ms-replicacion-actividades**. Este servicio permitirá grabar la información dentro de las tablas de Dynamo del sistema de Banco Digital.

Integración con sistemas externos

- Para actualizar la información tanto en el Core de Cuentas como en el Core de Clientes, los servicios del banco digital se integran con dos sistemas externos mediante el servicio **ms-integraciones-bancarias**.

Servicios de transferencias:

- El Sistema de Banco Digital ofrecerá diversas opciones para transferencias de dinero entre cuentas. Estas operaciones se realizarán a través de los siguientes servicios:

- Ms-recarga-dinero: Este servicio se utilizará para realizar ingresos de dinero en la cuenta de un usuario en el Banco Digital.
- Ms-retiro-dinero: Este servicio permitirá realizar retiros de dinero de la cuenta del usuario en el Banco Digital.
- Ms-transferencias-p2p: Este servicio permitirá realizar transferencias de dinero entre usuarios del Banco Digital.
- Ms-transferencias-interbancarias: Este servicio permitirá realizar transferencias de dinero entre otros bancos.
- Ms-billetera-tarjeta-virtual: Este servicio permitirá crear una tarjeta virtual al Banco Digital.

Servicio de notificaciones:

- El servicio de notificaciones, ms-notificaciones, se encarga de manejar las notificaciones del Banco Digital y utiliza el componente SNS de AWS para enviar notificaciones a través de PUSH, SMS y correo electrónico. Para las notificaciones PUSH, se utilizará Firebase. Además, se tiene previsto utilizar el componente externo Braze, que es más completo y permitirá un mejor seguimiento de las notificaciones.

Control de calidad:

- El control de calidad se gestionará mediante el uso de dashboards y el almacenamiento adecuado de registros en los trazos (logs) de AWS CloudWatch en un aplicativo AWS. De esta forma, se podrá monitorear el rendimiento del aplicativo y detectar posibles errores o fallas en el sistema.

Seguridad:

- El aplicativo contará con tokens para el consumo de los servicios que estarán expuestos. Además, se utilizará encriptación para proteger la información confidencial y garantizar la seguridad de los usuarios. Se utilizará el servicio Secret Manager de AWS para gestionar las credenciales de las APIs del Banco Digital, lo que garantiza la seguridad y protección de las credenciales y facilita su gestión y actualización en caso de ser necesario.

Arquitectura de microservicios:

- Los microservicios estarán alojados en contenedores administrados en Kubernetes. Para su comunicación, se utilizarán tópicos Kafka mediante eventos, lo que permitirá una comunicación efectiva y en tiempo real entre los diferentes microservicios, lo que ayudará a que el aplicativo sea escalable y flexible.

Proceso de Onboarding:

- Para el proceso de Onboarding, se contarán con los siguientes servicios:
  - Ms-biometria-facial: Este servicio se encargará de validar pruebas de vida

a través del proveedor FacePhi y consultará la data en el registro civil de los clientes.

- Ms-cuentas-virtual: Este servicio será el encargado de comunicarse con el sistema Core del Banco para crear las nuevas cuentas del Banco Digital.

Servicio de secuencia de pagos:

- El servicio ms-secuencia-pago contendrá una secuencia única que será utilizada como identificador único para las transferencias. De esta manera, se garantiza que cada transferencia tenga un identificador único y se facilite su seguimiento y gestión en el sistema.

Gestión de auditorías:

- Para la gestión de las auditorías en AWS, se utilizará la herramienta Kinesis. Con esta herramienta, se podrá administrar de forma efectiva y eficiente toda la información relacionada con las auditorías, lo que permitirá un seguimiento y gestión adecuados de las mismas.

Gestión de Dashboard de Logs en producción:

- Para el monitoreo de la aplicación en producción, se utilizará la herramienta Grafana para visualizar y analizar los registros (logs) generados por la aplicación y los servicios en AWS. De esta manera, se podrá detectar y solucionar cualquier problema en tiempo real, lo que garantizará la disponibilidad y estabilidad del sistema para los clientes. Además, se podrán realizar análisis históricos de la data de los clientes para mejorar el rendimiento y la eficiencia del aplicativo.

Activación de Trace Logs en CloudWatch

- Se utilizarán los Trace Logs de AWS CloudWatch para realizar un seguimiento detallado de las transacciones y operaciones realizadas por los usuarios en el aplicativo del Banco Digital. Esto permitirá detectar y solucionar rápidamente cualquier problema o incidencia en el sistema, lo que mejorará la calidad del servicio y la experiencia del usuario. Además, se podrá realizar un análisis profundo de la información registrada en los Trace Logs para mejorar la eficiencia y eficacia del sistema.

Gestión de uso de ElasticCache

- Se utilizará ElasticCache para mejorar el rendimiento y la escalabilidad del sistema, mediante la implementación de una capa de caché que permitirá almacenar datos en memoria y reducir la latencia de las operaciones de lectura y escritura en la base de datos. De esta manera, se logrará mejorar la experiencia del usuario y reducir los costos operativos.

Gestión de uso de ConfigMaps

- Se utilizarán ConfigMaps para almacenar variables de configuración y parámetros de los microservicios alojados en Kubernetes. Estos ConfigMaps permitirán modificar de forma centralizada la configuración de los microservicios sin necesidad de cambiar el código fuente de los mismos, lo que facilitará la gestión y el mantenimiento del sistema.

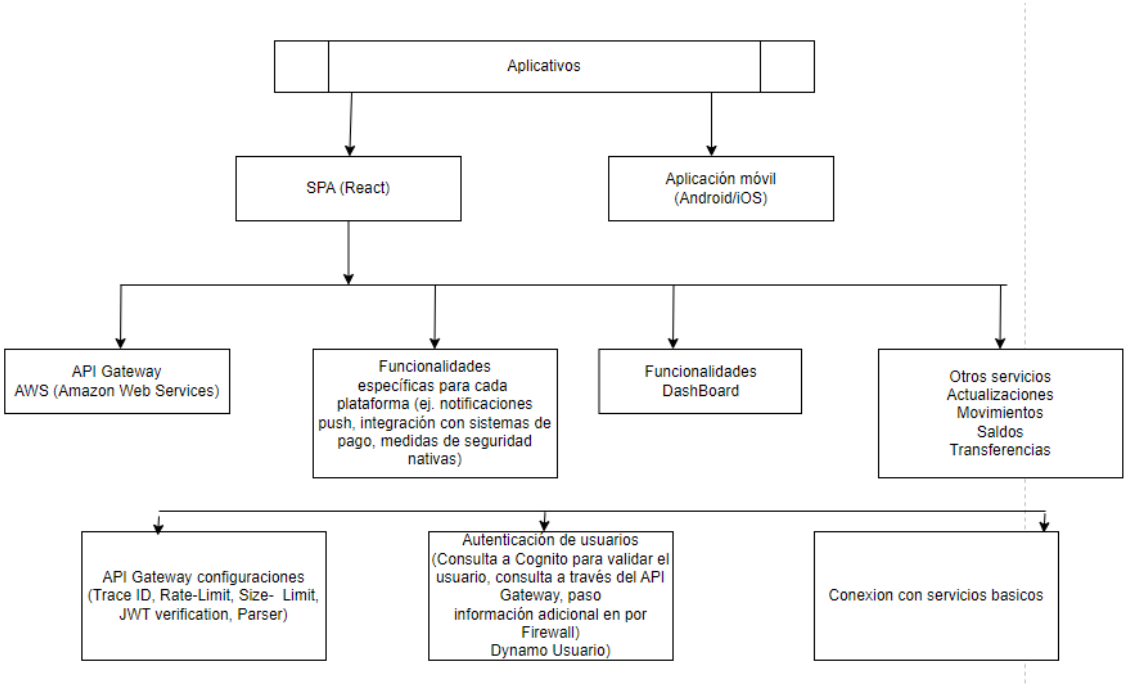
Gestión de uso de X-Ray

- Se utilizará X-Ray para rastrear y analizar el rendimiento de los servicios y microservicios del Banco Digital. Esto permitirá obtener información detallada sobre las llamadas realizadas a los servicios, los tiempos de respuesta, los errores y los cuellos de botella en el sistema. Además, con X-Ray se podrá visualizar el flujo de las llamadas entre los servicios y obtener información útil para la optimización del sistema y la mejora de la experiencia del usuario.

Gestión de uso de ScretManager

- En el proceso de despliegue y gestión de la aplicación, se utilizará el servicio de SecretManager de AWS para almacenar y administrar las credenciales y claves de acceso necesarias para el correcto funcionamiento de la aplicación. De esta forma, se asegura la protección de la información confidencial y se facilita la gestión y actualización de las credenciales en caso de ser necesario. Además, el servicio de SecretManager permite una gestión centralizada de las credenciales y su integración con otros servicios de AWS, como EC2, ECS y Lambda.

Diagrama de Contexto



Este diagrama de contexto representa los componentes que se mencionan en la descripción del sistema. El centro del diagrama es la sección de "Aplicativos", que incluye dos aplicativos: una SPA (React) y una aplicación móvil (Android/iOS).

Ambos aplicativos se comunican con los servicios del Banco Digital a través del API Gateway, que está expuesto en AWS. Los servicios públicos en AWS se conectan a través del Firewall antes de acceder al API Gateway.

El API Gateway tiene varias configuraciones importantes, como Trace ID, Rate-Limit, Size-Limit, JWT verification y Parser. Estas configuraciones aseguran la autenticación y la gestión del tráfico de los servicios.

El proceso de autenticación de usuarios se realiza mediante un servicio ms-autenticacion-usuario, que consulta la información del usuario en Cognito y en la tabla de Dynamo Usuario.

La sección de "Funcionalidades específicas para cada plataforma" representa las características únicas que se implementarán en cada aplicativo, como notificaciones push para dispositivos móviles, integración con sistemas de pago como Apple Pay o Google Pay y medidas de seguridad nativas como FaceID o TouchID en dispositivos de Apple.

La sección de "Dashboard" muestra cómo se mostrará la información del usuario, como los movimientos de la cuenta y el saldo, a través del servicio bff-consulta-saldos.

En caso de que el cliente realice transacciones desde otro canal que no sea el aplicativo móvil, el Core del Banco enviará las actualizaciones de movimientos y saldos a través de un servicio expuesto en AWS.

Los servicios web en el Core del Banco, que están expuestos a través de la herramienta