



EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA



Tecnológico Nacional de México

Instituto Tecnológico de Zacatecas

Adrián Aguilar Caldera

Administración de servicios en la nube

Servicios AWS.

Alexis Miguel Bracamontes Amaro 20450653

Enrique Alfonso Gómez Gómez 20450658

María Guadalupe Rivas Cervantes 20450660

Jeovanh Emmanuel Amaro Carlos 20450746

Jorge Hernández Ríos 20450659

Octubre 25 del 2024

Introducción.

En el contexto actual de la tecnología de la información, los servicios en la nube se han convertido en un pilar fundamental para el desarrollo y operación de sistemas y aplicaciones. Amazon Web Services (AWS) es uno de los líderes del mercado en este ámbito, ofreciendo una vasta gama de servicios que permiten a las organizaciones implementar, gestionar y escalar infraestructuras tecnológicas de forma eficiente y segura. Entre estos servicios, destacan soluciones clave como Amazon VPC, que facilita la creación de redes privadas virtuales, Amazon SQS para la gestión de colas de mensajes, y Amazon SNS para notificaciones masivas en tiempo real. Además, herramientas como API Gateway y AWS SWF proporcionan capacidades para gestionar la interacción de aplicaciones mediante APIs y flujos de trabajo complejos. Este conjunto de servicios es fundamental para instituciones y empresas que buscan optimizar sus sistemas TIC, aprovechando la escalabilidad, seguridad y flexibilidad que AWS pone a disposición. En esta introducción se exploran las principales características de estos servicios, así como los criterios que guían a los expertos en la selección de las soluciones más adecuadas para cada caso de uso.

Desarrollo.

Idea: Servicios AWS.

Competencia específica para desarrollar:

Conoce e identifica los distintos servicios que se pueden implementar en la nube.

Retos:

Conoceremos los servicios AWS (VPC Red privada en AWS, SQS Servicio de colas de mensajes, SWF Servicios de flujo de trabajo, SNS Servicio de notificaciones y API gateway).

Preguntas guía:

¿Cuáles servicios ofrece AWS para el funcionamiento de las TIC'S de la institución?

Amazon Web Services (AWS) ofrece una amplia gama de servicios que pueden ser utilizados para soportar las Tecnologías de la Información y la Comunicación (TIC) en una institución. Aquí tienes algunos de los principales:

- Amazon EC2 (Elastic Compute Cloud).

Proporciona capacidad de cómputo escalable en la nube. Permite ejecutar aplicaciones en servidores virtuales configurados según las necesidades específicas de la institución, ajustando la capacidad según la demanda.

- Amazon S3 (Simple Storage Service).

Ofrece almacenamiento de objetos escalable y seguro para almacenar datos críticos de la institución, como archivos, documentos y backups.

- Amazon RDS (Relational Database Service).

Servicio gestionado de bases de datos relacionales. Es útil para manejar bases de datos importantes para la operación de aplicaciones como sistemas de gestión académica o financiera.

- AWS Lambda.

Servicio de computación sin servidor que permite ejecutar código en respuesta a eventos sin gestionar servidores, ideal para tareas automáticas, como procesar datos o notificaciones.

- Amazon VPC (Virtual Private Cloud).

Permite crear una red privada virtual para gestionar recursos en la nube de manera segura, simulando un entorno de red propio.

- Amazon WorkSpaces.

Proporciona escritorios virtuales en la nube. Esto facilita que empleados y estudiantes accedan a escritorios virtuales desde cualquier lugar, mejorando la movilidad y flexibilidad del trabajo o aprendizaje.

- Amazon CloudFront.

Servicio de distribución de contenido que puede entregar recursos como sitios web, videos, o archivos de manera rápida y segura a usuarios globales.

- AWS IAM (Identity and Access Management).

Gestión de usuarios y control de acceso a recursos de AWS. Es vital para la seguridad y la administración de los permisos en una institución.

- Amazon SNS (Simple Notification Service).

Servicio de mensajería que puede enviar notificaciones a los usuarios de la institución a través de SMS, email, o aplicaciones móviles.

- AWS CloudFormation.

Permite automatizar el aprovisionamiento de infraestructura mediante plantillas, lo que facilita la gestión y réplica de recursos.

Estos servicios permiten mejorar la infraestructura TIC de una institución en cuanto a escalabilidad, seguridad, flexibilidad y costos, ajustándose a sus necesidades específicas.

Actividades guía:

Campo laboral.

Pregunta esencial:

¿Cuáles son los criterios que usan los expertos en TIC'S para elegir los servicios AWS para el funcionamiento de la infraestructura de TIC'S de la institución?

1. Conoceremos los recursos guía campo laboral.

Al elegir los servicios de AWS para el funcionamiento de la infraestructura de TIC's de una institución, los expertos en tecnología suelen considerar varios criterios clave para asegurarse de que los servicios seleccionados se alineen con los objetivos, requerimientos técnicos, y presupuestos de la organización. Aquí están los criterios más importantes:

1. Escalabilidad

Criterio: Capacidad de los servicios para manejar un crecimiento en la carga de trabajo o en el número de usuarios sin pérdida de rendimiento.

2. Disponibilidad y Confiabilidad

Criterio: Garantía de que los servicios estarán disponibles de manera ininterrumpida y funcionarán de forma fiable.

3. Seguridad

Criterio: Capacidad de los servicios para proteger datos sensibles y cumplir con regulaciones de seguridad.

4. Costo y Optimización de Recursos

Criterio: Relación entre los costos y el valor obtenido, así como la posibilidad de ajustar los servicios para no pagar por recursos innecesarios.

5. Facilidad de Integración

Criterio: Cómo de fácil es integrar los servicios de AWS con los sistemas y tecnologías ya existentes en la institución.

6. Flexibilidad

Criterio: Capacidad de los servicios para adaptarse a diferentes cargas de trabajo y necesidades.

7. Cumplimiento Normativo

Criterio: Capacidad de AWS para cumplir con las regulaciones específicas de la industria o el país.

8. Soporte Técnico y Formación

Criterio: Nivel de soporte técnico y formación disponible para los equipos de TI de la institución.

9. Rendimiento

Criterio: Capacidad del servicio para ofrecer una alta velocidad de procesamiento y baja latencia.

10. Automatización y Gestión Simplificada

Criterio: Disponibilidad de herramientas para automatizar la administración de la infraestructura.

11. Innovación y Nuevas Tecnologías

Criterio: Disponibilidad de servicios avanzados que permitan a la institución adoptar nuevas tecnologías.

12. Capacidad de Mantenimiento y Escalabilidad Internacional

Criterio: Posibilidad de expandir la infraestructura a nivel global si es necesario.

13. Facilidad de Uso y Herramientas de Desarrollo

Criterio: Simplicidad de la plataforma y las herramientas para su uso por el equipo de desarrollo de la institución.

Estos criterios permiten a los expertos en TIC seleccionar los servicios más adecuados para implementar una infraestructura tecnológica robusta, segura y eficiente. Dependiendo de las prioridades y los requerimientos específicos de la institución, algunos criterios pueden tener más peso que otros.

Palabras Clave:

Servicios AWS.

Amazon Web Services (AWS) es una plataforma de servicios en la nube que ofrece una amplia variedad de soluciones tecnológicas diseñadas para ayudar a empresas, instituciones y desarrolladores a gestionar, almacenar y procesar datos de manera eficiente y escalable. AWS proporciona infraestructura y herramientas bajo un modelo de "pago por uso", lo que permite a las organizaciones acceder a recursos informáticos sin la necesidad de invertir en hardware costoso o mantener infraestructura física propia.

Principales Tipos de Servicios de AWS:

1. **Cómputo:** AWS ofrece recursos de cómputo bajo demanda para ejecutar aplicaciones y gestionar cargas de trabajo de manera escalable. Amazon EC2 (Elastic Compute Cloud) permite a los usuarios lanzar instancias de servidores virtuales configurados a medida, mientras que AWS Lambda ofrece un modelo sin servidor que ejecuta código solo cuando es necesario, sin necesidad de gestionar servidores.
2. **Almacenamiento:** AWS proporciona soluciones de almacenamiento seguras y escalables para guardar y recuperar datos. Amazon S3 (Simple Storage Service) es un servicio popular que permite almacenar grandes cantidades de datos en diferentes formatos. También está Amazon EBS (Elastic Block Store) para almacenamiento en bloque, utilizado comúnmente junto con EC2 para bases de datos y aplicaciones empresariales.
3. **Bases de Datos:** AWS ofrece servicios gestionados de bases de datos para diferentes tipos de datos y cargas de trabajo. Amazon RDS (Relational Database Service) soporta bases de datos relacionales como MySQL, PostgreSQL y SQL Server. También ofrece Amazon DynamoDB, una base de datos NoSQL totalmente gestionada.
4. **Redes:** Amazon VPC (Virtual Private Cloud) permite a los usuarios crear redes privadas aisladas dentro de AWS, asegurando un entorno controlado y seguro para aplicaciones y datos. Además, AWS ofrece servicios como Elastic Load Balancing para distribuir el tráfico entrante y AWS Direct Connect, que permite conexiones dedicadas desde los centros de datos a AWS.

5. Seguridad: AWS integra la seguridad en todos sus servicios, ofreciendo herramientas como AWS IAM (Identity and Access Management), que permite gestionar permisos y accesos a recursos, y AWS KMS (Key Management Service) para cifrar datos. También cumple con estándares de seguridad globales como GDPR, HIPAA, y ISO.
6. Desarrollo y Automatización: AWS cuenta con herramientas para simplificar el ciclo de vida del desarrollo de aplicaciones. AWS CodePipeline y AWS Elastic Beanstalk permiten desplegar y gestionar aplicaciones sin preocuparse por la infraestructura subyacente. AWS CloudFormation facilita la automatización del aprovisionamiento de infraestructura mediante plantillas.
7. Machine Learning y Análisis de Datos: AWS ofrece soluciones avanzadas para el análisis de grandes cantidades de datos y la implementación de inteligencia artificial y machine learning. Amazon SageMaker permite construir, entrenar y desplegar modelos de machine learning de forma rápida. Servicios como Amazon Redshift ofrecen almacenamiento y análisis de datos a escala masiva.
8. Servicios de Contenedores: AWS es compatible con aplicaciones basadas en contenedores. Amazon ECS (Elastic Container Service) y Amazon EKS (Elastic Kubernetes Service) facilitan la ejecución y gestión de contenedores Docker y Kubernetes.
9. Content Delivery y CDN: Para entregar contenido a usuarios de manera rápida y eficiente, Amazon CloudFront permite distribuir contenido como sitios web, videos y aplicaciones a nivel global a través de una red de distribución (CDN) con baja latencia y alta transferencia de datos.
10. IoT (Internet of Things): AWS proporciona servicios como AWS IoT Core, que permiten la gestión y conexión de dispositivos IoT, recolectando datos y ejecutando aplicaciones basadas en la nube.

VPC Red privada en AWS.

Amazon Virtual Private Cloud (VPC) es un servicio de AWS que permite crear redes privadas dentro de la nube de AWS, proporcionando un entorno controlado y aislado donde los recursos de la nube, como instancias de EC2 y bases de datos, pueden operar de manera segura. Con VPC, puedes definir la estructura de red en la nube como si estuvieras gestionando una red en un centro de datos propio, pero con las ventajas y flexibilidad de la nube.

Características Principales de AWS VPC:

Aislamiento y Control Total:

AWS VPC permite crear una red privada virtual completamente aislada del resto de los usuarios de AWS. Tienes control total sobre el rango de direcciones IP, la configuración de subredes, la asignación de gateways, y las tablas de enrutamiento.

Subredes Públicas y Privadas:

Puedes dividir tu VPC en subredes públicas y subredes privadas. Las subredes públicas están conectadas a Internet a través de un Internet Gateway, permitiendo que los recursos sean accesibles desde fuera. Por otro lado, las subredes privadas se configuran sin acceso directo a Internet, protegiendo los recursos más sensibles de tu infraestructura.

Control de Enrutamiento:

VPC te permite configurar tablas de enrutamiento para controlar el tráfico de red entre subredes, y determinar qué subredes tienen acceso a Internet o a otras redes.

Seguridad con Listas de Control de Acceso (ACL) y Grupos de Seguridad:

AWS VPC ofrece mecanismos de seguridad a nivel de red. Los grupos de seguridad actúan como firewalls que controlan el tráfico entrante y saliente de instancias específicas, mientras que las listas de control de acceso de red (ACL) permiten gestionar el tráfico a nivel de subredes, lo que añade una capa adicional de seguridad.

Peering de VPC:

AWS permite conectar dos VPC diferentes mediante VPC Peering, lo que facilita la comunicación entre redes privadas en diferentes regiones o cuentas sin necesidad de usar la Internet pública.

VPN (Virtual Private Network) y AWS Direct Connect:

Puedes establecer una VPN para conectar tu infraestructura on-premise con tu VPC en AWS, creando una conexión segura y cifrada a través de Internet. Si necesitas mayor velocidad y seguridad, AWS Direct Connect proporciona una conexión privada dedicada desde tu red física a AWS.

Network Address Translation (NAT):

Para permitir que los recursos en subredes privadas accedan a Internet sin ser accesibles desde fuera, AWS VPC soporta dispositivos NAT (Network Address Translation), que permiten que instancias en subredes privadas puedan iniciar tráfico saliente a Internet sin exponer su dirección IP.

Gateways (Internet Gateway y NAT Gateway):

Internet Gateway (IGW) conecta tu VPC a Internet, permitiendo que las instancias en subredes públicas sean accesibles desde fuera. Por otro lado, NAT Gateway se utiliza para que instancias en subredes privadas puedan acceder a Internet para tareas como actualizaciones de software, sin hacerlas visibles a Internet.

Logs y Monitoreo:

AWS VPC se integra con Amazon CloudWatch y VPC Flow Logs, lo que te permite monitorear y registrar el tráfico de red de tus instancias. Esto es útil para auditoría, análisis de seguridad y resolución de problemas.

Ventajas de AWS VPC:

Seguridad Mejorada: AWS VPC ofrece un entorno completamente aislado con herramientas avanzadas de control de acceso y enrutamiento, lo que permite implementar arquitecturas de red seguras.

Escalabilidad: VPC te permite escalar recursos dentro de tu red privada a medida que crece tu infraestructura en la nube, sin necesidad de rediseñar la red completa.

Flexibilidad: Puedes diseñar la red de acuerdo con tus necesidades específicas, gestionando IPs, rutas y configuraciones de seguridad de manera granular.

Costos Reducidos: No es necesario invertir en infraestructura física para crear y mantener redes seguras. Todo se gestiona y paga según uso en AWS.

Interconexión con otras redes: Con servicios como VPC Peering y VPN, es sencillo conectar tu red privada en AWS con otras VPC o con redes externas, manteniendo la seguridad y el control.

Casos de Uso de AWS VPC:

Aislamiento de Aplicaciones Sensibles: Las aplicaciones que manejan información crítica pueden colocarse en subredes privadas dentro de una VPC, protegidas del acceso directo a Internet, lo que aumenta la seguridad.

Extensión de Infraestructura Local a la Nube: Muchas instituciones y empresas utilizan AWS VPC para extender sus centros de datos on-premise hacia la nube mediante VPN o AWS Direct Connect, mejorando la flexibilidad sin comprometer la seguridad.

Implementación de Servicios en la Nube con Mayor Control: Los desarrolladores que requieren un control granular sobre su red (rango de IPs, firewalls, enrutamiento) pueden utilizar AWS VPC para diseñar redes altamente personalizadas.

SQS Servicio de colas de mensajes.

Amazon SQS (Simple Queue Service) es un servicio de AWS que facilita la gestión de colas de mensajes, permitiendo que los sistemas distribuidos, aplicaciones o microservicios se comuniquen de manera asíncrona. SQS ayuda a desacoplar componentes de una arquitectura, lo que mejora la escalabilidad, flexibilidad y tolerancia a fallos al evitar la dependencia directa entre los diferentes servicios.

Características de Amazon SQS:

Desacoplamiento de Componentes:

SQS permite que los productores (que envían mensajes) y los consumidores (que procesan mensajes) trabajen de manera independiente. Esto asegura que una parte del sistema no dependa directamente de la otra para funcionar, lo que mejora la resiliencia y flexibilidad del sistema.

Gestión de Colas:

SQS gestiona las colas de mensajes en la nube, almacenando mensajes temporalmente hasta que los sistemas o servicios estén listos para procesarlos. Los mensajes se envían a las colas y luego se consumen en el orden que se reciben (FIFO) o en cualquier orden (standard).

Tipos de Colas:

Colas estándar: Este tipo de cola ofrece una alta tasa de entrega de mensajes y garantiza que cada mensaje se entregará al menos una vez, aunque no necesariamente en orden exacto.

Colas FIFO (First-In-First-Out): Garantizan que los mensajes se procesen en el orden en que fueron enviados y que cada mensaje se entregue exactamente una vez, lo que es esencial para aplicaciones donde el orden es importante.

Escalabilidad Automática:

SQS escala automáticamente para manejar cualquier cantidad de mensajes, sin necesidad de intervención del usuario. Esto es útil en sistemas donde la carga de trabajo varía considerablemente en diferentes momentos.

Duración y Retención de Mensajes:

Los mensajes se pueden retener en la cola hasta por 14 días. Esto permite a los sistemas recuperarse de fallos y procesar los mensajes en un momento posterior sin perder datos.

Entrega Segura:

SQS soporta la encriptación de mensajes utilizando AWS Key Management Service (KMS), lo que asegura que los datos en tránsito y en reposo estén protegidos. También permite definir políticas de acceso para garantizar que solo las entidades autorizadas puedan interactuar con la cola.

Modelos de Mensajería Asíncronos:

En sistemas donde no se necesita una respuesta inmediata, SQS permite enviar y recibir mensajes sin bloquear los procesos. Esto mejora la eficiencia en sistemas distribuidos, donde los servicios no tienen que estar sincronizados.

Visibilidad y Eliminación de Mensajes:

Una vez que un mensaje es leído por un consumidor, entra en un estado de "invisibilidad" durante un período de tiempo especificado. Si no se procesa dentro de ese tiempo, vuelve a estar visible en la cola para ser procesado nuevamente. Esto garantiza que los mensajes se procesen, incluso si un servicio falla temporalmente.

Ventajas de Amazon SQS:

Alta disponibilidad: SQS está diseñado para ser altamente disponible y ofrecer un servicio fiable sin necesidad de gestionar la infraestructura subyacente.

Desacoplamiento y resiliencia: Permite que los sistemas distribuidos funcionen de manera más independiente, lo que aumenta la tolerancia a fallos.

Escalabilidad: Escala automáticamente según la carga de trabajo sin necesidad de configuración adicional.

Costo-efectivo: Al usar un modelo de pago por uso, SQS permite gestionar grandes cantidades de mensajes sin incurrir en altos costos.

Casos de Uso de Amazon SQS:

Procesamiento de Tareas en Lotes:

Aplicaciones que necesitan procesar grandes volúmenes de tareas pueden enviar los trabajos a una cola y permitir que los consumidores los procesen a su propio ritmo, mejorando la eficiencia.

Desacoplamiento de Microservicios:

En arquitecturas de microservicios, SQS es útil para desacoplar servicios, lo que permite que cada servicio se enfoque en una tarea específica sin necesidad de esperar o depender de otros servicios.

Gestión de Flujos de Trabajo:

En flujos de trabajo donde las tareas necesitan ser procesadas en un orden específico, las colas FIFO de SQS aseguran que los mensajes se procesen en el orden correcto, lo que es crítico en procesos como la aprobación de transacciones o el procesamiento de pedidos.

Aplicaciones de Alto Rendimiento:

En aplicaciones con grandes volúmenes de transacciones o eventos (como comercio electrónico o sistemas bancarios), SQS asegura que los mensajes no se pierdan, incluso bajo carga alta, lo que garantiza la integridad del sistema.

Integración con Otros Servicios AWS:

Amazon SNS (Simple Notification Service): SQS se puede integrar con SNS para recibir notificaciones y eventos de otras partes de la arquitectura.

AWS Lambda: SQS puede desencadenar funciones de Lambda para procesar mensajes de manera automática sin la necesidad de gestionar servidores.

Amazon S3 y DynamoDB: SQS puede recibir notificaciones de cambios en S3 o DynamoDB, lo que permite procesar eventos en tiempo real.

SWF Servicios de flujo de trabajo.

Amazon SWF (Simple Workflow Service) es un servicio de AWS diseñado para ayudar a los desarrolladores a coordinar tareas dentro de aplicaciones distribuidas. SWF facilita la creación y gestión de flujos de trabajo complejos al permitir la definición y el seguimiento de una serie de actividades o pasos en procesos empresariales y aplicaciones automatizadas. Es ideal para coordinar tareas que requieren procesamiento distribuido, larga duración, y alta fiabilidad.

Características de Amazon SWF:

Coordinación de Tareas:

Amazon SWF permite dividir una aplicación o proceso en varias actividades (tasks) y decisiones (decision tasks) que pueden ejecutarse en diferentes servicios o máquinas. Las actividades representan el trabajo que debe realizarse, mientras que las decisiones determinan la siguiente actividad a ejecutar en función de los resultados anteriores.

Estado de los Flujos de Trabajo:

SWF mantiene el estado y progreso de cada flujo de trabajo de manera confiable, lo que permite supervisar qué actividades han sido completadas, cuáles están en progreso y qué tareas necesitan reiniciarse en caso de fallos.

Duración Extendida:

Amazon SWF permite la gestión de flujos de trabajo que pueden durar desde minutos hasta meses. Esto lo hace adecuado para procesos empresariales de larga duración, como la gestión de pedidos, la cadena de suministro o la coordinación de proyectos complejos.

Gestión de Errores:

SWF detecta fallos y garantiza que las tareas incompletas o fallidas se reinicien, permitiendo una alta tolerancia a fallos en el sistema sin la intervención del usuario. Esto asegura que los procesos se completen de manera confiable.

Separación de Lógica de Control y Lógica de Trabajo:

SWF separa la lógica de control de flujo de trabajo (coordinación y toma de decisiones) de la lógica de trabajo (tareas reales), lo que permite una mayor flexibilidad y claridad al desarrollar aplicaciones distribuidas. Esto facilita la gestión de procesos complejos sin que los desarrolladores deban implementar su propio sistema de gestión de flujo.

Seguimiento y Monitoreo:

Con Amazon SWF, se puede monitorear el estado de cada tarea y obtener informes detallados sobre el progreso del flujo de trabajo. Esto es útil para realizar auditorías, solucionar problemas y optimizar el desempeño de los procesos.

Escalabilidad y Alta Disponibilidad:

Amazon SWF escala automáticamente para manejar una gran cantidad de flujos de trabajo simultáneamente, sin que los desarrolladores necesiten preocuparse por la infraestructura subyacente.

Roles en SWF:

SWF tiene tres roles principales:

Workflow Starter: Inicia un flujo de trabajo (como una orden de compra).

Decider: Toma decisiones basadas en los resultados de las actividades previas (por ejemplo, si un pago es aprobado, el siguiente paso puede ser el envío).

Activity Worker: Realiza las tareas reales (como la ejecución de un pago o el envío de un correo electrónico).

Ventajas de Amazon SWF:

Automatización y Coordinación:

SWF simplifica la automatización de procesos empresariales al coordinar las diferentes partes del flujo de trabajo, lo que facilita el manejo de tareas distribuidas de larga duración sin intervención manual.

Alta Fiabilidad:

Al encargarse de la gestión de fallos y reinicios de tareas fallidas, SWF asegura que los flujos de trabajo se completen correctamente incluso si hay errores o interrupciones.

Flexibilidad:

Se puede utilizar en una amplia gama de aplicaciones, desde procesamiento en lotes hasta sistemas críticos de negocio que requieren monitoreo constante, como sistemas financieros, sistemas de logística o plataformas de comercio electrónico.

Integración con Otros Servicios AWS:

SWF se integra con otros servicios de AWS, como Amazon EC2, AWS Lambda y Amazon S3, lo que permite crear flujos de trabajo más complejos y eficaces.

Escalabilidad Dinámica:

El servicio está diseñado para escalar automáticamente según la carga de trabajo, lo que lo hace adecuado para entornos con alta concurrencia de flujos de trabajo o procesos a gran escala.

Casos de Uso de Amazon SWF:

Procesamiento de Pedidos:

SWF se puede utilizar para gestionar y coordinar el procesamiento de pedidos en línea. Cada pedido puede tener un flujo de trabajo que incluye actividades como la validación del pago, la gestión del inventario, el envío del producto y la notificación al cliente.

Gestión de Proyectos:

En proyectos complejos que involucran múltiples equipos y tareas, SWF puede coordinar el trabajo distribuyendo tareas, rastreando el progreso y garantizando que se completen en el orden correcto.

Procesos de Aprobación:

SWF se utiliza para gestionar flujos de trabajo en los que diferentes pasos de aprobación son necesarios, como aprobaciones legales, financieras o de gestión de productos, asegurando que el flujo se realice de manera secuencial y sin errores.

Procesos de Machine Learning:

En proyectos de machine learning, SWF puede gestionar la secuencia de actividades necesarias para la recopilación de datos, el preprocesamiento, el entrenamiento de modelos y la evaluación.

SNS Servicio de notificaciones.

Amazon SNS (Simple Notification Service) es un servicio de mensajería completamente administrado que facilita la entrega de notificaciones a través de diferentes protocolos como HTTP/HTTPS, SMS, correo electrónico, o a otros servicios de AWS como Amazon SQS o AWS Lambda. SNS permite la entrega rápida y flexible de mensajes, ideal para aplicaciones distribuidas, notificaciones en tiempo real, y coordinación entre sistemas.

Características de Amazon SNS:

Publicación/Suscripción (Pub/Sub):

SNS sigue el modelo de mensajería de publicación/suscripción, en el que un emisor (publicador) envía un mensaje a un tema, y los receptores (suscriptores) que están registrados en ese tema reciben el mensaje. Esto permite una comunicación asíncrona y distribuida.

Entrega a Múltiples Protocolo:

SNS admite una variedad de protocolos para la entrega de mensajes, incluyendo:

HTTP/HTTPS: Los mensajes se envían a un endpoint de URL.

Amazon SQS: Los mensajes pueden entregarse a una cola de SQS para procesamiento posterior.

AWS Lambda: SNS puede activar funciones Lambda en respuesta a eventos, lo que permite la ejecución de código sin servidores.

Correo electrónico y SMS: SNS también puede enviar mensajes directamente a direcciones de correo electrónico o números de teléfono móvil vía SMS.

Alta Disponibilidad y Escalabilidad:

Amazon SNS es un servicio completamente administrado que escala automáticamente para manejar grandes volúmenes de mensajes, asegurando una entrega fiable y de baja latencia, incluso cuando se incrementan los niveles de tráfico.

Filtrado de Mensajes:

SNS permite a los suscriptores filtrar los mensajes que desean recibir en función de los atributos del mensaje. Esto optimiza el uso de recursos y asegura que cada suscriptor solo reciba los mensajes que le interesan.

Temas:

Los temas en SNS actúan como canales a los que los publicadores envían mensajes. Los suscriptores se inscriben a estos temas para recibir los mensajes pertinentes. Esto permite una organización eficiente de la entrega de notificaciones según diferentes propósitos.

Entrega Fiable:

SNS asegura la entrega fiable de mensajes utilizando mecanismos de reintento en caso de fallos. Los suscriptores de protocolos como HTTP/HTTPS recibirán reintentos si el endpoint no está disponible inicialmente.

Encriptación y Seguridad:

SNS admite la encriptación de mensajes en tránsito y en reposo mediante AWS Key Management Service (KMS), lo que garantiza que los mensajes están protegidos mientras se envían o almacenan.

También es posible configurar políticas de acceso que limiten quién puede publicar o suscribirse a temas específicos, mejorando la seguridad.

Monitorización con CloudWatch:

Amazon SNS se integra con Amazon CloudWatch, permitiendo a los usuarios monitorear la actividad de los temas y obtener métricas detalladas sobre el rendimiento, como el número de mensajes enviados y fallos de entrega.

Ventajas de Amazon SNS:

Entrega en Tiempo Real:

SNS garantiza la entrega de notificaciones en tiempo real a una amplia variedad de destinatarios, lo que lo hace adecuado para sistemas que requieren notificaciones inmediatas, como aplicaciones móviles o sistemas de monitoreo.

Desacoplamiento de Componentes:

SNS permite que los componentes de una arquitectura distribuyan los mensajes de manera asíncrona, lo que mejora la escalabilidad y la resiliencia de la aplicación. Los publicadores no necesitan saber quién o cuántos son los suscriptores, lo que facilita el crecimiento del sistema.

Fácil de Usar y Administrar:

Amazon SNS es fácil de configurar y no requiere infraestructura adicional, lo que permite a los desarrolladores enfocarse en la lógica de negocio sin preocuparse por la gestión del sistema de mensajería.

Escalabilidad Automática:

El servicio maneja cualquier cantidad de mensajes sin necesidad de intervención manual, escalando automáticamente para ajustarse a las demandas de tráfico.

Costo-Efectivo:

SNS utiliza un modelo de pago por uso, en el que solo se paga por el número de publicaciones y el número de notificaciones entregadas, lo que lo hace económico para una variedad de casos de uso.

Casos de Uso de Amazon SNS:

Notificaciones Push para Aplicaciones Móviles:

SNS se utiliza para enviar notificaciones push a dispositivos móviles a través de servicios como Apple Push Notification Service (APNS) o Google Cloud Messaging (GCM), lo que permite a las aplicaciones móviles mantener a los usuarios actualizados en tiempo real.

Coordinación de Microservicios:

En arquitecturas de microservicios, SNS se usa para orquestar la comunicación entre servicios distribuidos. Un servicio puede enviar un mensaje a un tema SNS, y varios otros servicios suscritos a ese tema pueden reaccionar a la notificación de manera autónoma.

Notificaciones Automáticas para Eventos en AWS:

SNS puede ser integrado con otros servicios de AWS para enviar notificaciones automáticas cuando ocurren ciertos eventos, como cambios en el estado de una instancia de EC2 o la finalización de un trabajo de procesamiento de datos en Amazon S3.

Sistemas de Alertas y Monitoreo:

SNS es útil para implementar sistemas de alertas que notifican a administradores y equipos de soporte cuando se detectan problemas o eventos críticos en la infraestructura. Las alertas se pueden enviar por correo electrónico, SMS o integrarse con sistemas de gestión de incidentes.

Envío Masivo de Mensajes:

SNS es ideal para enviar mensajes a un gran número de destinatarios, como campañas de marketing, recordatorios de eventos o actualizaciones importantes para los usuarios de una aplicación.

Comparación con Otros Servicios AWS:

Amazon SQS: Mientras que SQS es un servicio de cola de mensajes que permite comunicación asíncrona y almacenamiento de mensajes para su posterior procesamiento, SNS está diseñado para la entrega inmediata de notificaciones a múltiples suscriptores simultáneamente.

AWS Lambda: SNS puede invocar funciones de Lambda en respuesta a eventos, permitiendo la ejecución automática de código en función de los mensajes recibidos.

API gateway.

Amazon API Gateway es un servicio de AWS que permite a los desarrolladores crear, publicar, mantener, monitorear y asegurar APIs a cualquier escala. API Gateway facilita la creación de APIs RESTful y WebSocket para que los desarrolladores puedan exponer funciones o servicios backend a aplicaciones cliente, como aplicaciones web, móviles o IoT. Su integración con otros servicios de AWS, como AWS Lambda, Amazon EC2, y Amazon S3, lo convierte en una herramienta poderosa para crear arquitecturas serverless y de microservicios.

Características de Amazon API Gateway:

Creación de APIs RESTful y WebSocket:

API Gateway permite crear APIs REST que siguen el estilo de arquitectura de transferencia de estado representacional (RESTful), lo que facilita la interacción entre aplicaciones cliente y los servicios backend. También permite crear APIs WebSocket, ideales para aplicaciones que requieren comunicación bidireccional en tiempo real, como aplicaciones de chat o de trading financiero.

Integración con Servicios Backend:

API Gateway puede interactuar con diversos backend, como funciones de AWS Lambda, instancias de Amazon EC2, Amazon S3, Amazon DynamoDB, y otros servicios HTTP o HTTPS. Esto permite que las APIs sirvan como una capa intermedia para acceder a lógica empresarial y almacenamiento de datos.

Gestión del Ciclo de Vida de la API:

El servicio facilita la publicación de nuevas versiones de APIs y la gestión de diferentes etapas del ciclo de vida, como desarrollo, prueba, y producción, lo que permite iterar y mejorar las APIs de manera estructurada.

Seguridad:

API Gateway proporciona múltiples mecanismos de seguridad, como la autenticación y autorización mediante AWS Identity and Access Management (IAM), Amazon Cognito, y autenticación basada en OAuth 2.0. También permite limitar el acceso a las APIs mediante claves de API, lo que garantiza que solo los usuarios autorizados puedan interactuar con los endpoints.

Escalabilidad Automática:

API Gateway está diseñado para manejar miles de solicitudes simultáneas y escalar automáticamente para ajustarse a la carga sin necesidad de intervención manual, lo que lo hace adecuado para aplicaciones que experimentan picos de tráfico.

Gestión del Tráfico y Throttling:

API Gateway permite establecer límites de tasa y políticas de aceleración (throttling) para controlar el tráfico entrante a las APIs. Esto es crucial para evitar sobrecargar los servicios backend y garantizar la calidad del servicio.

Monitoreo y Análisis:

Se integra con Amazon CloudWatch, lo que permite obtener métricas, logs y alarmas sobre el rendimiento de las APIs. Los desarrolladores pueden monitorear el uso de la API, la latencia, los errores, y otras métricas críticas para mantener la calidad del servicio.

Manejo de Versiones y Etapas:

Los desarrolladores pueden manejar diferentes versiones de una API, cada una asignada a distintas etapas, como desarrollo, prueba y producción. Esto permite la iteración continua y la implementación segura de nuevas funcionalidades.

Transformación de Solicitudes y Respuestas:

API Gateway ofrece capacidades para modificar y transformar tanto las solicitudes entrantes como las respuestas salientes. Esto permite adaptar las APIs a los requisitos específicos de los clientes o los servicios backend, como formatear los datos o aplicar encabezados personalizados.

Soporte para CORS (Cross-Origin Resource Sharing):

API Gateway soporta el manejo de CORS, lo que permite que los clientes de diferentes dominios accedan a las APIs de manera segura. Esto es esencial para habilitar la interacción entre aplicaciones web y APIs.

Ventajas de Amazon API Gateway:

Desarrollo Ágil:

API Gateway permite a los desarrolladores exponer rápidamente funcionalidades backend como APIs, facilitando un desarrollo ágil y la rápida implementación de nuevas características.

Escalabilidad y Disponibilidad:

Al estar totalmente administrado por AWS, API Gateway escala automáticamente para manejar grandes volúmenes de tráfico, proporcionando alta disponibilidad sin la necesidad de gestionar servidores.

Costos Reducidos:

API Gateway sigue un modelo de pago por uso, donde los desarrolladores solo pagan por las solicitudes realizadas a la API y no por el tiempo o la infraestructura de servidores. Esto lo hace especialmente rentable para aplicaciones que tienen fluctuaciones en la carga de trabajo.

Integración Serverless:

API Gateway se integra perfectamente con AWS Lambda, lo que permite crear arquitecturas serverless donde no es necesario gestionar servidores. Esto reduce la complejidad operativa y los costos asociados.

Control Granular de Seguridad y Acceso:

Proporciona control detallado sobre quién puede acceder a las APIs y cómo, gracias a la integración con servicios de autenticación como Amazon Cognito y IAM, lo que garantiza un alto nivel de seguridad.

Experiencia del Cliente Personalizada:

Gracias a las transformaciones de solicitudes y respuestas, los desarrolladores pueden personalizar la interacción con los clientes, ajustando las respuestas del backend según las necesidades del cliente sin modificar el código del servidor.

Casos de Uso de Amazon API Gateway:

Exposición de Microservicios:

API Gateway es ideal para crear una capa de API que exponga varios microservicios distribuidos. Cada microservicio puede estar respaldado por diferentes tecnologías, como funciones Lambda, contenedores en ECS o instancias EC2, y API Gateway puede centralizar y coordinar estas interacciones.

APIs para Aplicaciones Móviles y Web:

Las aplicaciones móviles y web pueden utilizar API Gateway para interactuar con los servicios backend. Esto permite manejar autenticación, autorización y la entrega de datos de manera centralizada.

Creación de Aplicaciones Serverless:

En arquitecturas serverless, API Gateway se utiliza en conjunto con AWS Lambda para manejar solicitudes HTTP y ejecutar lógica empresarial sin servidores dedicados. Esto es ideal para aplicaciones de bajo costo y alto rendimiento.

Integración de Dispositivos IoT:

Las APIs creadas con API Gateway pueden facilitar la comunicación entre dispositivos IoT y backend, lo que permite a los dispositivos interactuar de manera segura y eficiente con servicios en la nube.

Puerta de Entrada a Big Data:

API Gateway puede servir como puerta de entrada para la ingestión de grandes volúmenes de datos desde diversas fuentes hacia servicios como Amazon S3 o Amazon Kinesis, lo que facilita la recolección y procesamiento de datos a gran escala.

Diferencia entre API Gateway y Otros Servicios de AWS:

AWS Lambda: API Gateway es la interfaz frontend que permite a los clientes hacer solicitudes HTTP a los backend, mientras que Lambda es el servicio que ejecuta código en respuesta a esas solicitudes. API Gateway gestiona el enrutamiento y la autenticación, mientras que Lambda gestiona la ejecución del código.

Amazon Elastic Load Balancing (ELB): ELB distribuye tráfico a instancias EC2 u otros servicios backend, pero no proporciona las características de seguridad, transformación de solicitudes, ni la flexibilidad de API Gateway para gestionar APIs RESTful.

Nota: Con la experiencia que se adquirió, elaboraremos un sólo **reporte en equipo** de autoría propia (**especifica quién hizo que**) donde **subraya las palabras clave**, con extensión de una cuartilla en formato pdf con la nomenclatura: **CL_SA_NO_DEEQUIPO** y lo enviaremos al e-mail: adseln@itz.edu.mx, durante nuestra hora de clase.

Conclusiones:

En conclusión, la adopción de servicios en la nube de Amazon Web Services (AWS) proporciona a las organizaciones una plataforma robusta y escalable para optimizar su infraestructura de Tecnologías de la Información y Comunicación (TIC). Servicios como Amazon VPC, SQS, SNS, SWF y API Gateway permiten a las instituciones diseñar arquitecturas eficientes que facilitan la comunicación entre componentes, la gestión de mensajes y la implementación de APIs, lo que se traduce en un aumento significativo de la agilidad y la innovación. La capacidad de AWS para escalar automáticamente y su enfoque en la seguridad hacen que estas soluciones sean ideales para satisfacer las demandas de entornos empresariales en constante evolución. Además, la flexibilidad para integrar diferentes servicios backend, junto con herramientas de monitoreo y análisis, permite a los desarrolladores gestionar y optimizar continuamente sus aplicaciones. A medida que las organizaciones continúan explorando y aprovechando el potencial de AWS, es evidente que estos servicios no solo mejoran la eficiencia operativa, sino que también impulsan la transformación digital, preparando a las instituciones para enfrentar los retos del futuro.

Referencias:

[Welcome to AWS Documentation.](#)