Universidad ORT Uruguay
Facultad de Ingeniería

Infraestructura en la nube 1

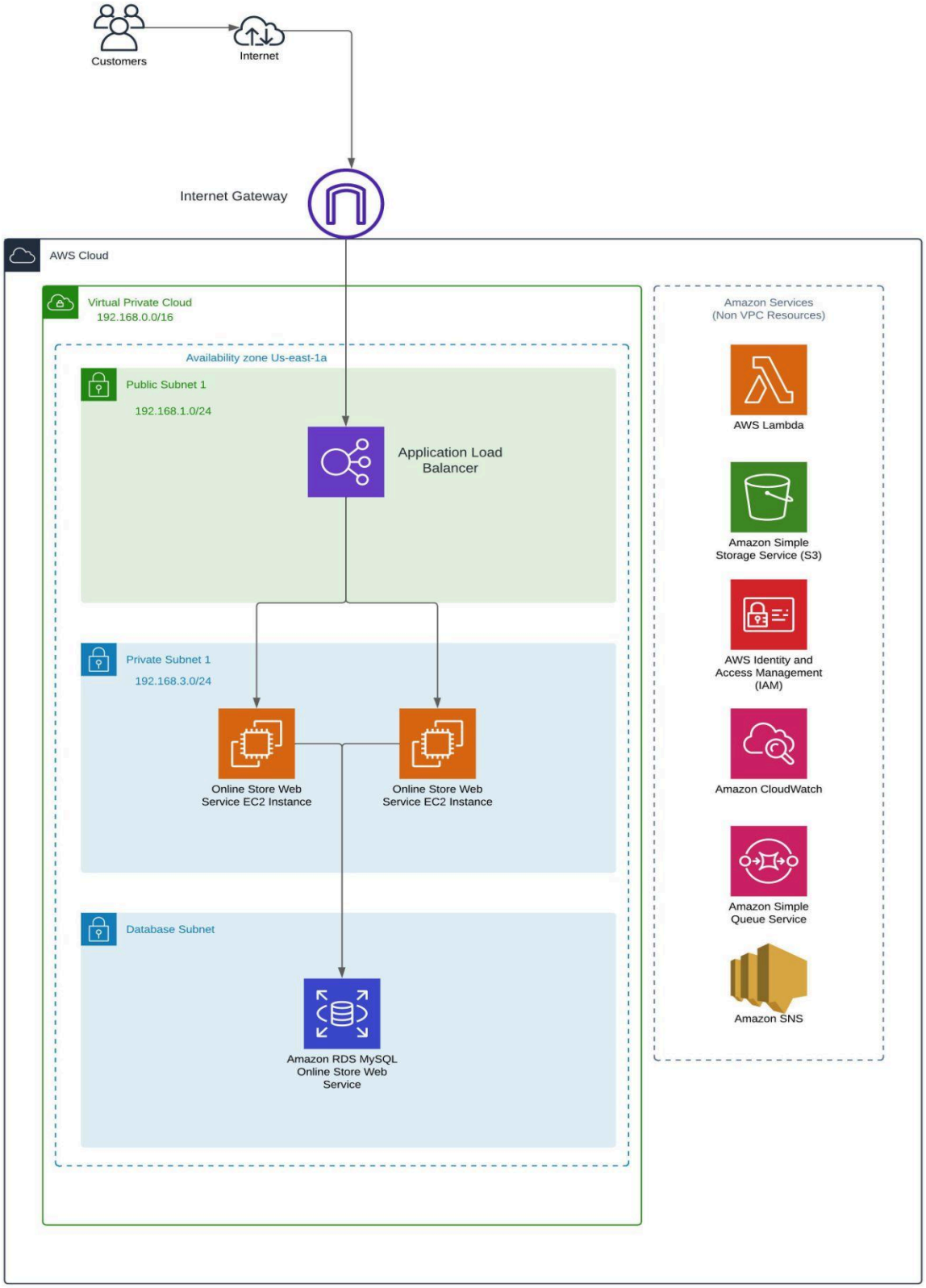
Obligatorio 2

Guillermo Scheck - 221910

2024

Diagrama de la Infraestructura

VPC


Customers
Internet
Internet Gateway
AWS Cloud
Virtual Private Cloud
192.168.0.0/16
Availability zone Us-east-1a
Public Subnet 1
192.168.1.0/24
Application Load Balancer
Private Subnet 1
192.168.3.0/24
Online Store Web Service EC2 Instance
Online Store Web Service EC2 Instance
Database Subnet
Amazon RDS MySQL Online Store Web Service
Amazon Services (Non VPC Resources)
AWS Lambda
Amazon Simple Storage Service (S3)
AWS Identity and Access Management (IAM)
Amazon CloudWatch
Amazon Simple Queue Service
Amazon SNS

Componentes

Internet Gateway (IGW):

- Permite la comunicación entre la VPC y el internet. De esta manera los usuarios pueden acceder a la aplicación web.

Application Load Balancer (ALB):

- Distribuye el tráfico entrante entre las instancias de EC2 en las subredes privadas, asegurando alta disponibilidad y escalabilidad horizontal.

Subred Pública:

- Contiene el ALB, permitiendo que el tráfico desde internet llegue a las instancias de EC2.

Subred Privada:

- Contiene las instancias EC2 donde se ejecuta el servicio web. Estas instancias no son accesibles directamente desde internet, aumentando la seguridad.

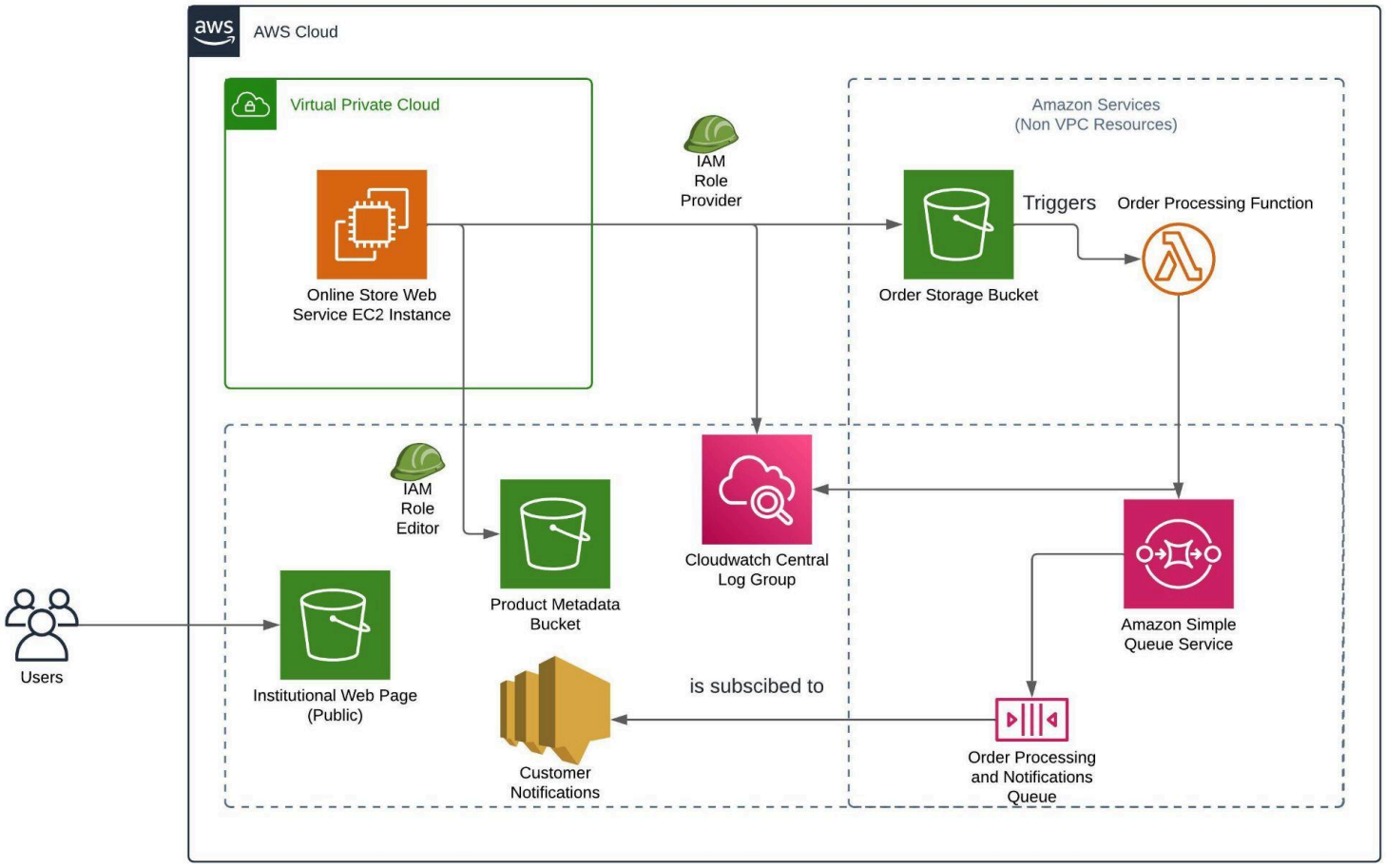
Subred de Base de Datos:

- Contiene la instancia de Amazon RDS (MySQL). Esta configuración asegura que la base de datos esté en una red privada y no sea accesible desde internet, proporcionando una capa adicional de seguridad.

Servicios no vinculados a la VPC:

- **AWS Lambda:** Para el procesamiento de órdenes de manera automática
- **Amazon S3:** Almacenamiento de metadata para productos, almacenamiento de órdenes, seguimiento de una página web estática.
- **IAM:** Gestión de permisos y roles para la interacción entre los servicios.
- **CloudWatch:** Monitoreo y logging centralizado en un solo grupo
- **SQS y SNS:** Gestión de colas para el procesamiento de órdenes y notificaciones.

Servicios AWS en acción



Componentes

EC2 Instances:

- Ejecución del servicio web en la VPC, conectado a otros recursos mediante roles de IAM.

IAM Roles:

- **Provider:** Permite a las instancias de EC2 realizar operaciones sobre el bucket de almacenamiento de órdenes.
- **Editor:** Permite a las instancias de EC2 realizar operaciones sobre el bucket de almacenamiento de datos de los productos.

Amazon S3 Buckets:

- **Order Storage Bucket:** Encargado de almacenar las órdenes subidas por los proveedores.
- **Product Metadata Bucket:** Encargado de almacenar todo lo referente a los datos de los productos.
- **Institutional Web Page Bucket:** Almacena la página web institucional, accesible públicamente.

AWS Lambda:

- Procesa eventos desde el bucket de almacenamiento de órdenes. Cuando un proveedor sube una orden, esta función de dispara, enviando esta orden a la cola de órdenes y notificaciones para un posterior procesamiento,

Amazon CloudWatch:

- Centralizar logs y métricas para monitorear la aplicación.

Amazon SQS:

- Gestiona las colas de procesamiento de órdenes y notificaciones.

SNS:

- Envío desacoplado de notificaciones a los clientes.

Cumplimiento de los Requerimientos del Negocio

Alta Disponibilidad y Escalabilidad para el servicio web:

- La utilización de un ALB para distribuir el tráfico entre múltiples instancias EC2 asegura que la aplicación pueda escalar horizontalmente y mantenerse disponible en caso de falla de una instancia.

Seguridad

- Aunque no está explícitamente mencionado, este detalle nunca está de más. La colocación de las instancias de base de datos y del servicio web en subredes privadas, junto con el uso de roles de IAM para controlar el acceso a los recursos, son buenas prácticas que contribuyen a un estado seguro de los mismos.

Desacoplamiento de Servicios de Notificación/Mensajería:

- El uso de Amazon SQS y SNS para manejar las notificaciones y mensajería hacia los clientes. Al emplear SQS, las notificaciones se colocan en una cola y se procesan de manera asincrónica, lo que asegura que las notificaciones no se pierdan, aunque no lleguen instantáneamente. Esto cumple con el requerimiento del cliente de desacoplar estos servicios de los sistemas web, garantizando la entrega confiable sin necesidad de inmediatez.

Procesamiento de Órdenes:

- La utilización de S3, Lambda, y SQS para procesar y manejar las órdenes hace de esto un proceso totalmente automático, que no requiere de intervención manual alguna y que solo se activa cuando realmente se lo necesita.

Monitoreo y Logging:

- Usando CloudWatch, se proporciona un grupo de logs genérico. Este permite un monitoreo centralizado, ayudando a mantener la visibilidad sobre la salud y el rendimiento de la aplicación.

Aspectos a mejorar

Uso del script user data.sh para inicializar un servidor web "template":

- Esta estrategia no es la más adecuada ni la más común en el uso de la herramienta. Se utilizó esta estrategia para automatizar al máximo el proceso de levantar la infraestructura para el profesor. Idealmente, se debería haber seguido la parte opcional de la tarea, donde se desarrolla un proceso que automáticamente despliega los servicios cuando se sube el código a algún artefacto.

Automatización del módulo principal de Terraform:

- El módulo principal podría automatizarse aún más, iterando la ejecución de módulos. Por ejemplo, sobre la cantidad de recursos presentes en las "configs" en vez de tener que escribir un módulo nuevo cada vez. Esto es un tradeoff entre claridad, mantenibilidad y facilidad de desplegar nuevos recursos. Para dejar en claro en el código los recursos que decidí construir, este enfoque fue el más conveniente.

Uso de un módulo genérico IAM:

- El uso de un módulo genérico IAM para crear un rol y asociarlo a políticas quizás no fue realmente necesario. Para este caso, era parte de la infraestructura y se considera más como normas que se deben seguir para cumplir con los atributos más importantes. Por tanto, quizás dejar esta parte como acciones de otros módulos no hubiera estado mal.