Asignatura: OPC13 – Cloud Computing

Ensayo de resultados de aprendizaje de la **semana 12**

Temas: IAM, Networking, Compute, Storage, Security, Governance and Administration

Integrantes:

Adrian Caleb Jaramillo Flores
Matrícula: 367857
a367857@uach.mx

Ana Rebeca Moreno Reza
Matrícula: 367783
a367783@uach.mx

Abel González Mireles
Matrícula: 361031
a361031@uach.mx

Miguel David Rodríguez González.
Matrícula: 343786
a343786@uach.mx

Docente:

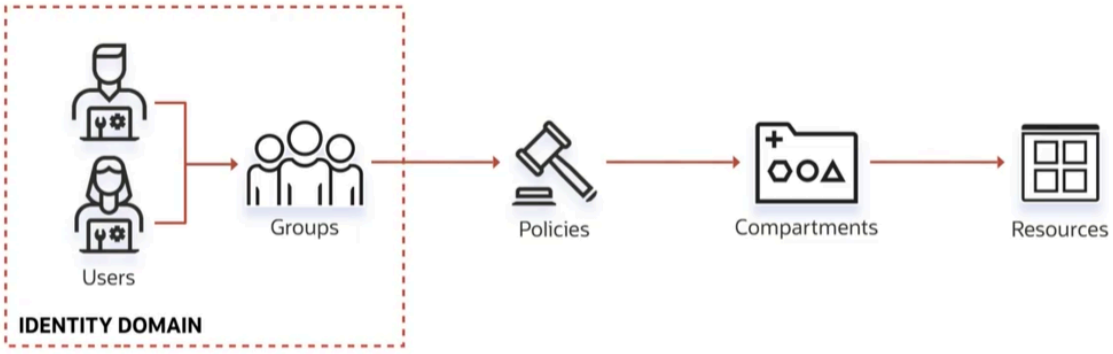
David Maloof Flores
Matrícula: 197589
a197589@uach.mx

1. Resumen Tema "IAM"

IAM se refiere a Identity and Access Management Service (Servicio de manejo de acceso e identidad), este se basa en dos ideas principales, la primera es ***AuthN*** que se refiere a la identidad del usuario, ¿Quién eres? Usuario introduce credenciales (usuario/contraseña, MFA, clave de API, etc.). La segunda es ***AuthZ*** la cual se pregunta qué permisos o roles tiene disponible el usuario/grupo, ¿Qué se te permite hacer? Se verifica la existencia de una Política IAM que asigne el permiso al Grupo/Principal sobre el recurso en el Compartimento.

Primero te **autenticas** (AuthN) para probar tu identidad, y luego el sistema te **autoriza** (AuthZ) para realizar tareas basadas en tus permisos.

La primera información clave son los dominios de identidad, estos son contenedores de identidad que te permiten gestionar usuarios, grupos, aplicaciones y configuraciones de seguridad asociadas a ellos mismos, cada dominio es indiferente de los demás, es decir, tienen su propia configuración, políticas y opciones de autenticación.



Otro dato clave son los ***Compartments*** estos se usan con el fin de organizar y aislar recursos en la nube (Máquinas virtuales, redes, bases de datos, almacenamiento, …) con el fin de organizar los recursos (por ejemplo: Desarrollo, Producción, Pruebas, TI, Finanzas, …) y para tener un control de acceso a estos recursos donde las políticas definen las acciones que podrán realizar los usuarios o grupos sobre los recursos que se tienen en el compartimiento. PD. No se puede usar un mismo recurso en dos compartimientos pero si se puede anidar varios compartimentos dentro de sí mismos (máximo 6 anidamientos).

Otros términos que son esenciales en IAM son los:

Principals (Entidades de seguridad) que se refiere a una entidad en OCI (Oracle Cloud Infraestructure) a la que se le puede conceder acceso a los recursos. Esencialmente, es "quién" puede interactuar con los servicios en la nube (

IAM Users - Personas individuales o aplicaciones que necesitan acceder a la consola o API de OCI (Generalmente usan usuario/contraseña o claves de API y son persistentes),

Instance Principals - Permite que instancias como las Virtual Machine hagan llamadas a las API de OCI sin tener que configurar credenciales de usuario,

Dynamic groups - Agrupación especial de recursos (como instancias de VM o bases de datos) que se definen por un conjunto de reglas, si un recurso coincide con la regla, se agrega al grupo y obtiene sus permisos).

Groups son colecciones de usuarios IAM que evitan la necesidad de asignar políticas a cada usuario individualmente, algo interesante es que un usuario puede permanecer en varios grupos y heredar los permisos de todos ellos.

Tenancy se refiere a tu cuenta principal y aislada en OCI; Es la entidad raíz de todos los recursos y la base para la facturación.

Tenancy setup se refiere a las tareas iniciales y de mejores prácticas realizadas al configurar tu cuenta por primera vez, las cuales son cruciales para la seguridad y la organización (por ejemplo:

Root Compartment (Compartimento Raíz): Todo Arrendamiento tiene un compartimento raíz implícito. Por convención, es una buena práctica no poner la mayoría de tus recursos en el compartimento raíz.

Creación del Primer Administrador: El primer usuario IAM creado durante el registro es el administrador predeterminado del Arrendamiento (tiene acceso total)

Estructura de Compartimentos: Crear una estructura inicial de **Compartimentos** (ej. Desarrollo, Pruebas, Producción) para aislar recursos y establecer límites de seguridad).

2. **Resumen Tema "Networking"**

Ahora, en el tema de Networking tenemos distintos conceptos clave que se deben conocer, estos son:

VCN (Virtual Cloud Network) que se refiere a tu red privada y personalizable en la nube. Es el equivalente virtual de una red de centro de datos tradicional donde se tiene un control total sobre el direccionamiento IP, las subredes, las tablas de rutas y los cortafuegos.

comunnication permite la comunicación ***Intra-VCN*** (el tráfico entre subredes de una misma VCN se maneja de manera automática por el propio enrutamiento local de OCI y debido a esto no requiere reglas explícitas en las tablas de rutas para que las subredes se puedan comunicar entre sí), así como también por medio de ***comunicación externa*** (Requiere de un *Gateway* y reglas en la *tabla de rutas*;

el *Internet Gateway* permite el acceso bidireccional entre las subredes públicas y la internet,

el *NAT Gateway*, permite que los recursos de las subredes privadas se puedan comunicar con internet pero no al revés,

Servicio Gateway, permite que los recursos de las subredes privadas accedan a servicios de OCI sin pasar por el internet).

Route Table se refiere al conjunto de reglas que se usarán para dirigir el tráfico que sale de cada subred o recurso hacia fuera de ellos:

- Cada subred debe estar asociada a una única tabla de rutas
- Las reglas de la tabla de rutas dirigen el tráfico hacia un **destino (**bloque CIDR, como 0.0.0.0/0 para internet**)** a través de un **target (**Gateway, NAT gateway o un DRG - *Dynamic routing gateway***)**

peering (interconexión) es el proceso de conectar dos VCN que se pueden llegar a comunicar usando direcciones IP privadas, lo que permite crear redes distribuidas y segmentadas.

- *Local peering*: Conecta dos VCN dentro de la misma región usando un **Local peering gateway (LPG).**
- *Remote peering:* Conecta dos VCN ubicadas en diferentes regiones de OCI usando Dynamic Routing Gateway (DRG) en la versión v2.

El ***Load Balancer*** se utiliza para lograr un alta disponibilidad y también para lograr escalabilidad, también se le conoce como **proxy inverso.** Algunas opciones de Load Balancers en OCI son: ***Layer 7 HTTP/S*** se presenta en dos unidades Escalable - Flexible y el segundo en Dinámicas donde no es necesario que el Load Balancer calcule**,** se puede realizar de manera pública y privada, también tiene una alta disponibilidad y funciones avanzadas. El segundo tipo es llamado ***Network Load Balancer*** funciona en Layer 4 TCP y UDP, tiene una opinión pública y privada, también tiene una alta escalabilidad y disponibilidad, es mas veloz (menor latencia) que HTTP/S LB, pero el HTTP/S LB tiene un nivel superior porque puede consultar paquetes, inspeccionarlos y obtener esa inteligencia.

3. Resumen Tema "Compute"

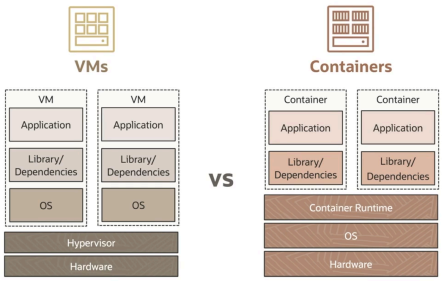
El servicio de OCI Compute ofrece Máquinas Virtuales y Bare Metal Machines (un servidor dedicado exclusivamente para un sólo usuario) o un Host Dedicado (Bare Metal Machine junto con máquinas virtuales) para los requerimientos de los cómputos o aplicaciones que se tengan. Tienen *escalabilidad, alto rendimiento* y un *costo bajo.*

OCI Compute ofrece la ***flexibilidad de formas***, lo que permite al usuario escoger los CPUs y memorias que se ajusten a sus necesidades. Al igual que permite escoger el procesador que el usuario desee.

También existen las ***instancias***, que son un host para cómputo. Oracle al igual que AWS tiene centros de datos llamados *Availability Domains*. La primera dependencia dentro del servicio de cómputo es una red cloud virtual dividida en subred. Otra dependencia es el volumen para bootear el sistema operativo. Además se utiliza *Live Migration* para migrar la máquina virtual en caso de fallos.

Un concepto importante en Compute es la ***escalabilidad***, de los cuales hay dos tipos: horizontal y vertical. *Escalar verticalmente* implica escalar una instancia hacia arriba o hacia abajo, dependiendo de lo que sea permitido por la forma de la instancia; además, la nueva forma de la instancia debe tener la misma arquitectura de hardware que la instancia original. Es recomendable detener una instancia antes de hacer escalamiento vertical. El *escalamiento horizontal* (o *autoscaling*) implica crear muchas máquinas virtuales con la misma forma, permitiendo la alta disponibilidad, ya que si una de las máquinas virtuales falla se puede utilizar alguna otra que sí esté funcionando.

Oracle también ofrece la posibilidad de usar contenedores, a continuación se muestra la diferencia entre un contenedor y una máquina virtual:



Oracle utiliza Kubernetes para el manejo de contenedores a través del Container Engine for Kubernetes (OKE).

4. **Resumen Tema "Storage"**

Existen diferentes requerimientos para el almacenamiento. Es importante tener definido si se requiere de un almacenamiento *persistente* (que se almacena de manera segura) o no persistente y también saber qué tipo de datos se quiere almacenar; además es importante saber qué rendimiento y capacidad son necesarias, junto con la durabilidad (hacer múltiples copias). Es necesario saber si los datos se almacenarán de manera local o externa.

OCI ofrece diversos servicios para el almacenamiento: *Local NVMe*, *Block Volume*, *File Storage*, *Object Storage*. Al igual que existen servicios para la migración de datos como *Data Transfer Disk* y *Data Transfer Appliance*.

- ***OCI Object Storage*** es una plataforma de alto rendimiento en la que los datos se almacenan como objetos, lo cual es ideal para datos no estructurados.
- ***OCI Block Volume*** provee almacenamiento persistente y durable a las instancias de cómputo.
- ***OCI File Storage*** funciona para aplicaciones de Oracle Lift and Shift, sistemas de propósito general para archivos, micro servicios y contenedores, Scale Out, analíticas.

5. **Resumen Tema "Security"**

Modelo de seguridad compartida:

En un entorno local, el usuario es dueño de todo el conjunto de lo que constituye sus instalaciones, incluyendo las responsabilidades que ésto conlleva, mientras más se acerca a la nube, algunas de éstas responsabilidades se traspasan al proveedor de servicios en la nube en cuestión, por lo que el modelo de seguridad compartida, hace referencia precisamente a compartir las responsabilidades en función de que tan cargado a la nube se encuentre el sistema. en el caso de Oracle, éste se responsabiliza por las cuestiones de seguridad en la nube, tales como, centros de datos físicos, centros de conexión físicos, hosts físicos y la capa de virtualización, asegurándose de que sea veloz y actualizada, mientras que el usuario es responsable de sus datos, dispositivos, cuentas e identificadores, aplicaciones, controles de red y sistema operativo en uso.

En el caso de OCI, respecto a la seguridad, se encuentra dividido en 5 capas, de las cuales, cada una cuenta con sus servicios específicos para intentar asegurar la seguridad de los usuarios

- Protección de infraestructura
    - Protección DDoS, Controles de seguridad de red, Firewalls virtuales, Filtros de tráfico de red malicioso
- Administración de acceso e identidad
    - Manejo de acceso a usuario y políticas, Manejo de autenticador multifactor, Inicio de sesión único para proveedores de identidad, grabado de llamadas al API de manera automática
- Protección de sobrecarga y sistema operativo
    - Arranque seguro, arranque medido, TPM, aislamiento de sobrecarga, parches de sistema operativo y manejo de paquetes
- Protección de datos
    - Encriptación de datos en reposo y tránsito, llave de almacenamiento centralizada y administración, Descubrir, clasificar y proteger datos
- Detección y remedio
    - Administración de manejo de seguridad, asesores de seguridad, Escaneos de exhibición y vulnerabilidad

6. Resumen Tema "Governance and Administration"

En Oracle se manejan las siguientes formas de pago: ***Pay as you go (*PAYG*)*** donde solo se paga lo que se usa. ***Annual Universal Credits*** en el cual el usuario se compromete con un plan anual de créditos, a cambio de este compromiso, se obtiene un ahorro considerable; aunque también hay una variación en el pago final dependiendo del consumo de estos créditos. ***Bring Your Own License (*BYOL*)*** este método es para los clientes que ejecutan licencias locales si desean utilizarlas en la nube, lo que reduce el costo general y puede reutilizar esas licencias en la nube. Los factores que más impactan al precio son: el tamaño de los recursos, transferencia de datos y el tipo de recurso.
OCI nos proporciona diferentes herramientas para gestionar los costos: ***OCI Budgets*** (crear presupuestos, y configurar alarmas para prevenir la superación del presupuesto)***, Cost Analysis***(Análisis del costo de los recursos usados, y así ver los cambios que se pueden hacer para reducir costos)***, Usage Reports***(Se generan diariamente, y son reportes en formato CSV)***, Service Limits and Usage***(Limita el uso de servicios y recursos, para no sobrepasar cuotas o tiempo de uso)***, Compartment Quotas***(Limita el uso de servicios y recursos)**.**

El ***tagging*** es una capacidad muy importante dentro de OCI. Son básicamente pares de valores clave, que puedes utilizar para organizar mejor los recursos, permite customizar la organización de nuestros recursos de una manera óptima y eficiente en donde el usuario pueda comprender lo hecho anteriormente, también ayuda a mejorar el manejo de los cotos

esto debido a que nos ayuda a identificar en qué tags se usan más recursos o genera más costos y modificarlo, y por último ayuda en el control de acceso, ya que al separarlo por tags puedes aplicar quien trabaje en cual tag y limitar su acceso solamente a ese o esos tags.

Existen dos implementaciones ***Free-form tags*** la cual es un implementación básica, solamente comprime llave y valor, y no tiene un esquema definido o una restricción de acceso. El segundo es la implementación recomendada ***Defined Tags*** tiene más control y funciones que el anterior, también se puede almacenar en Namespaces en el cual se pueden poner tantas etiquetas como desee en esos espacios, en base a lo dicho anteriormente se puede decir que se está definiendo un esquema, además es compatible con las políticas lo cual implementa una mejor seguridad.

Tag Namespace: Es un contenedor para un conjunto de tags key con tag key definitions.

Tag key definition: Especifica su llave y que tipos de valores son permitidos.

Ninguna de las dos puede ser eliminada, pero sí retirada.

Las recompensas de soporte son aquellas que ganan los clientes por medio del consumo de recursos, y luego se aplican como forma de pago para licencias de actualización de software y soporte para los programas de tecnología de Oracle, la visualización de estas recompensas se hacen de manera sencilla para tener acceso de una manera rápida y poder canjearlas a través de la consola.