Asignatura: OPC13 – Cloud Computing

Ensayo de resultados de aprendizaje de la **semana 14**

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

Integrantes:

Diego Pérez Prieto
Matrícula: 365341
a365341@uach.mx

Jared Alejandro Rosas Molina
Matrícula: 365337
a365337@uach.mx

1. Subtema "Identity and Access Management"

La gestión de identidad y acceso (IAM) es un servicio de OCI que controla de manera segura quién accede a los recursos, qué tipo de acceso tiene y a qué recursos específicos.

El proceso central ocurre en dos pasos, el primero se llama autenticación (también referido como AuthN) y el segundo se denomina autorización (AuthZ). La autenticación tiene que lidiar con verificar quién es alguien, es decir, identificar al usuario que entre a un sistema, mientras que la autorización se encarga de administrar qué permisos puede tener cada tipo de usuario.

Existen varios aspectos clave dentro de este tema, como los dominios de identidad, usuarios, grupos y políticas. Cada uno se define de la siguiente manera:

- Dominios de Identidad: Es donde viven los usuarios y grupos. Se encarga de la Autenticación (verificar quién eres) mediante contraseñas, Autenticación Multifactor (MFA) o Inicio de Sesión Único (SSO).
- Usuarios: Son las personas o aplicaciones del sistema.
- Grupos: Conjuntos de usuarios. Esta se considera la mejor manera de conceder permisos, no a usuarios individuales.
- Políticas: Son las reglas que definen la Autorización (qué puedes hacer).

Por último, otro concepto que se maneja en IAM son los "Compartments". Los compartimientos son carpetas que organizan y aíslan los recursos en la nube, como ejemplo estás las máquinas virtuales, redes o bases de datos. Se puede agrupar recursos por departamento (Ventas, finanzas) o por entorno (Producción, desarrollo). Además son un pilar de la seguridad, ya que las políticas se aplican a los compartimientos para definir qué grupos pueden gestionar los recursos dentro de ese compartimiento

2. Subtema “Networking”

El networking en OCI se basa en la VCN (Virtual Cloud Network), la red privada, aislada y segura en la nube donde se despliegan los recursos.

Dentro de una VCN, se crean subredes, que son divisiones del rango de IP (ej. 10.0.1.0/24) para organizar y aislar recursos. Las subredes pueden ser públicas (con acceso a internet) o privadas (aisladas). Para poder crear una VCN, OCI ofrece un asistente de creación, el cual provisiona automáticamente los componentes esenciales para la conectividad: un Internet Gateway, para permitir el tráfico hacia y desde la subred pública y un NAT Gateway para permitir que los recursos en la subred privada inicien conexiones a internet sin exponerlos a conexiones entrantes.

Una vez que la red está construida, la gestión del flujo de tráfico se vuelve primordial. Aquí es donde entra en juego el enrutamiento de la VCN. Cada subred se asocia con una Tabla de Ruta, que actúa como el sistema de navegación de la red. Estas tablas contienen reglas que dictan a dónde debe dirigirse el tráfico. Por ejemplo, una regla en la subred pública dirigirá todo el tráfico destinado a Internet (0.0.0.0/0) hacia el Internet Gateway, mientras que una regla en la subred privada dirigirá ese mismo tráfico al NAT Gateway.

Otro tema importante es la seguridad de la VCN, esto es vital y se implementa a través de un modelo de "defensa en profundidad" con dos tipos de firewalls virtuales. Primero, las Listas de Seguridad, que operan a nivel de subred y aplican un conjunto de reglas a todos los recursos dentro de esa subred. Después, los Grupos de Seguridad de Red, que ofrecen un control al aplicar reglas directamente a la tarjeta de red virtual de un recurso específico. Esto permite agrupar recursos con los mismos requisitos de seguridad independientemente de la subred en la que vengan.

Finalmente, para alta disponibilidad y escalabilidad, el Load Balancer (Balanceador de Carga) distribuye automáticamente el tráfico entrante entre servidores backend. Realiza "chequeos de salud" constantes para asegurar que solo envía tráfico a servidores operativos, redirigiendo el flujo si uno falla.

3. Subtema “Compute”

El servicio de Cómputo es el corazón de cualquier plataforma en la nube, ya que proporciona la potencia de procesamiento necesaria para ejecutar aplicaciones. En OCI, este servicio ofrece un amplio espectro de opciones, permitiendo a los usuarios elegir el modelo exacto que se ajusta a sus necesidades de rendimiento, costo y gestión. El cómputo en OCI se centra en su capacidad para ofrecer desde servidores físicos completos hasta entornos de ejecución sin servidor. Los usuarios pueden desplegar recursos de cómputo en cuestión de minutos, pagando solo por lo que utilizan.

Dentro del cómputo se maneja el concepto de instancia. Una "instancia" es un servidor virtual o físico en la nube. Al crear una, se deben definir dos componentes clave: la "forma", que determina los recursos asignados como OCPUs (CPUs de Oracle) y la cantidad de RAM, la "imagen", que es la plantilla del sistema operativo y el software que se instalará en el volumen de arranque de la instancia.

Una vez que una instancia está en funcionamiento, el escalado se vuelve crucial para manejar las fluctuaciones de la demanda. OCI ofrece dos métodos principales. El escalado vertical implica cambiar la "forma" de una instancia existente para darle más, o menos OCPU y RAM, lo cual es útil para cargas de trabajo que crecen de manera predecible. Más importante aún es el escalado horizontal que permite añadir o eliminar automáticamente instancias de un grupo basándose en métricas de rendimiento, como el uso de la CPU. Esto asegura que la aplicación tenga el rendimiento necesario durante los picos de demanda y ahorre costos durante los períodos que no se use.

Para cargas de trabajo más modernas y complejas, OCI ofrece el Oracle Container Engine for Kubernetes (OKE). Kubernetes es el estándar de la industria para la orquestación de contenedores, y OKE es el servicio gestionado de OCI que simplifica su despliegue y operación. En lugar de que los desarrolladores gestionen manualmente la compleja infraestructura de Kubernetes, OCI maneja el "plano de control", permitiendo a los equipos centrarse solo en desplegar sus aplicaciones.

Finalmente, el cómputo Serverless con Oracle Functions elimina la necesidad de gestionar infraestructura. Los desarrolladores cargan código como "funciones" individuales que responden a eventos específicos. OCI se encarga de ejecutar y escalar la función, cobrando solo por los milisegundos en que el código estuvo activo.

4. Subtema “Storage”

El tipo de almacenamiento que se quiere asignar dependerá completamente de distintos requisitos, desde el tipo de dato a almacenar, si serán persistentes o no, es decir que los datos se almacenan de forma segura, o si los datos serán duraderos, es decir, se crean distintas copias de un dato por si, en dado caso una copia sale mal se tienen otras copias de éste en la base de datos, a su vez, se necesitara saber la conectividad que se tendrá con los datos y que protocolo se utilizara el cual será diferente según la aplicación que se desarrollara. Existen distintos tipos de almacenamientos, como lo puede ser el Local NVMe, el cual cuenta con un servidor de cálculo y un almacenamiento asociado que usa SSD NVMe, además de éste existe el almacenamiento por objetos, almacenamiento por bloques y el almacenamiento por archivos.

En el almacenamiento por objetos, se puede almacenar distintos tipos de archivos, como lo son desde archivos de texto hasta archivos de video, este tipo de almacenamiento se

utiliza cuando se quiere tener un repositorio, cuando existen datos no estructurados o semi-estructurados, para big data o para fines como respaldos. Para identificar a un objeto se tiene una tupla de nombre – valor, donde el nombre es un ID del objeto y el valor será lo que contiene dicho objeto, del cual se puede encontrar sus metadatos, accediendo al objeto mediante una API con comandos de HTTP, además de que, el objeto se almacenara dentro de un bucket, éste debe de tener un nombre único dentro del servidor y de manera global y contiene una jerarquía plana. Dentro de este tipo de almacenamiento existen tres diferentes niveles, el nivel estándar, infrecuente y nivel de archivo, los cuales almacenaran datos dependiendo de su frecuencia de acceso, siendo el estándar con mayor frecuencia y el nivel de archivo el menos frecuente.

En el almacenamiento por bloques, una instancia se comunica con los bloques que contienen discos persistentes y duraderos encontrados en un servidor, dentro de estos se pueden asociar y conectar discos a las instancias o desvincularlas y eliminar los discos, o eliminar las instancias y mantener los datos independientemente del ciclo de vida de la instancia, haciéndolos persistentes y duraderos. Existen distintos niveles de este tipo de almacenamiento, como lo es el de bajo costo, balanceado, de rendimiento superior y de rendimiento ultraalto, los cuales, dependerán de si tienen un bajo o un alto nivel de demanda de entradas y salidas respectivamente.

El almacenamiento por archivos es una recopilación de documentos organizados en diferentes directorios de manera jerárquica, la cual consiste en dos o más instancias que comparten un almacenamiento que pueden escribir y leer archivos dentro de éste último, donde existen distintas distribuciones de sistemas de archivos, como lo es el NFS de Linux o SMB de Windows, este tipo de almacenamiento se utiliza para propósitos de compartir y guardar datos dentro de carpetas, para darle estado a microservicios y contenedores, entre otros

5. Subtema “Security”

El termino “Modelo de seguridad compartida” significa que, la responsabilidad de los datos recae tanto en el dueño de la aplicación desarrollada como en el proveedor del servicio de almacenamiento en la nube, donde el desarrollador tiene la responsabilidad de la seguridad de los datos, quienes acceden a estos y los que acceden que acciones pueden hacer con la información, mientras que la responsabilidad del proveedor es cuidar el centro físico de los datos, de la red, de los servidores y la virtualización de los datos. Existen diversos casos para el cual utilizar distintos servicios que ofrecen los proveedores, los cuales pueden ser para proteger la infraestructura, tener un manejo de las identidades y acceso de los usuarios, protección para los datos, protección para el sistema operativo y la zona de trabajo, entre otros.

OCI ofrece distintos servicios para la seguridad de los datos, como lo es Cloud Guard, el cual sirve para supervisar e identificar posibles amenazas y solucionarlos, donde la soución puede ser automatizada, para hacer esto se especifica un destino (ámbito de los recursos que se examinaran), luego se seleccionaran detectores los cuales identificaran problemas en las acciones de los usuarios o de los recursos usados, se notificara de los problemas y después se solucionara el problema con distintas acciones dependiendo de la amenaza.

La encriptación, es usada para transformar datos en un texto cifrado a traves de distintos numeros y letras aleatorias que no tienen sentido para la lectura mediante un algoritmo, pero para la encriptación sí, a lo cual se le llama "clave", mientras que el decifrado es el proceso inverso, utilizado para transformar el cifrado a datos que tengan sentido para el humano. La encriptación estatica, donde los datos estaticos almacenados en un servidor, base de datos o cuenta de almacenamiento no se pueden leer sin que se tenga la clave, mientras que la encriptación en transito, son datos que se mueven entre ubicaciones, donde durante el movimiento a traves de una red se encriptan los datos, teniendolos seguros mediante la transmisión de datos protegiendolos de atacantes externos. Algunos tipos de cifrado son el simetrico, donde se usa una sola llave para la encriptación y desencriptado de los datos, mientras que la encriptación asimetrica es aquella donde se usan diferentes llaves para la encriptación y el desencriptado.

Otro servicio ofrecido es OCI Vault, el cual permite manejar las claves de cifrado y otras credenciales, eliminando la necesidad de almacenar claves de cifrado y secretos en distintos archivos de configuración, donde las claves de cifrado son aquellas que permiten que el cifrado y descifrado de información, mientras que los secretos son las contraseñas, certificados, tokens de autenticación, etc. Esta protección se puede dar mediante software o hardware security modules (HSM), donde la diferencia es que, en HSM las operaciones criptograficas se quedaran en el dispositivo HSM y no se podran exportar, pero en software se guardaran en el servidor y se podran exportar. La encriptación de las llaves es con el cifrado de sobres, en la que existen claves para cifrar los archivos pero para mantenerlos seguros se cifran con otra clave maestra.

6. Subtema "Governance and Administration"

En OCI, los precios serán diferentes dependiendo del modelo que se utilice, un modelo es el "Pay as you go", en el que solamente se cobra los recursos utilizados los cuales son medidos, pero si se utilizan funciones no incluidas, se tiene que pagar por lo consumido aunque no se este utilizando, también está el modelo de Creditos universales anuales, donde se dan fondos por año con lo que se obtiene bastantes ahorros, pero se debe de utilizar la cantidad de creditos dados durante todo el año, un modelo similar a este es Credito universal mensual, y por último, existe el modelo de traer licencias propias, donde los desarrolladores pueden ejecutar dichas licencias en la nube reduciendo el costo. Existen diferentes factores por las cuales el precio puede subir o bajar, uno de ellos es la cantidad de recursos dados, donde mientras más sean los recursos más caro sera, otro factor es el

tipo de recurso que se quiere usar, además, un factor importante que puede aumentar el precio es la tranferencia de los datos, donde para ingresarlos no tiene costo pero para exportarlos sí.

Para manejar los costos, OCI ofrece distintas herramientas, una de ellas es OCI Budgets, con los que se realiza un seguimiento del presupuesto para un compartimento, donde se pueden configurar alertas que notificaran si se prevee que se superara el presupuesto o se supera éste último. Otra herramienta, es el analisis de costos, en el que se pueden ver los costos pasados y poder cambiar ciertos elementos para que el costo no sea tan grande según lo analizado. A su vez, la plataforma de OCI ofrece reportes de uso, los cuales se generan de manera diaria mostrando los datos de uso de cada recurso utilizado. También si se quiere definir los limites, las cuotas y el uso, OCI ofrece la herramient para hacerlo, liberandose de un uso indebido de los recursos. Aparte, existe la manera en que dentro de los compartimentos se puedan aislar recursos y tener un acceso a estos, pudiendo configurar cuotas de comportamiento. Además, OCI ofrece el programa de Oracle Support Reward, dandole un valor adicional a los clientes que utilizan su plataforma junto con sus servicios, obteniendo recompensas de soporte que se pueden aplicar como forma de pago para las licencias de actualización de software y soporte para los programas.

El etiquetado, es una función incluida dentro de OCI, el cual, es un par de clave (Id de la etiqueta) – valor (el que se desea asignar) utilziado para organizar los recursos, donde, principalmente se utiliza cuando se crean aplicaciones con arquitecturas complejas, pudiendo etiquetarlas para organizar los recursos dependiendo de que parte de la aplicación o que aplicación necesita más o menos, con esto se puede manejar los costos, ya que se sabe que etiqueta esta utilizando recursos de más, a su vez, se puede controlar el acceso a los recursos basandose en la etiqueta. Existen dos tipos de etiquetado, la primera es el formato libre, donde no hay un esquema especifico ni una restricción de acceso, mientras que en las etiquetas definidas, con estas se puede tener un mejor control, primeramente estas estan dentro de un espacio de nombres definiendo un esquema, donde el nombre de este esquema se puede asegurar con una politica teniendo un manejo de quien utiliza dichas etiquetas definidas.