Introducción a STORAGE (Almacenamiento)

Tenemos diferentes tipos de información, cada uno con sus particularidades(extensiones).

Todo esto vamos a ser capaces de almacenarlos en OCI.

Tipo de datos: Persistente vs No Persistente

Persistente: Queda almacenada a lo largo del tiempo

No Persistente: No queda almacenada por tanto tiempo

Rendimiento:

IOPS: Input/Output Operations Per Second (operaciones por segundo por entrada y salida). Ver el almacenamiento como un disco curo.

Capacidad de procesamiento.

Se puede acceder por un almacenamiento local,almacenamiento de red.

Existen diferentes protocolos para acceder a los datos: Block,File,HTTP

Tipos de almacenamiento que se tienen en Oracle

Memoria Rapida No volatil: Es un almacenamiento conectado localmente.

Volume Block: Tiene un mayor uso.

Persistente,durable,tamaño fijo.

File Storage

Se encuentra dentro de un dominio de disponibilidad

Se conforma por 2 instancias y se van a comunicar con una File Storage.

Object Storage

Es muy utilizado, poder almacenar fotos,videos,archivos de texto, musica,sitios web.

Vamos a tener comunicación entre la computadora y el internet

Metodo PUT (Poner o registrar)

Metodo GET (Obtener)

En una organización se guarda demasiada información.

Muchas aplicaciones almacenan datos y toda esa información que se guarda en los discos duros o servidores se migra a la nube.

Data Transfer Disk: Tomamos los discos y los enviamos a oracle, quien se encargara de subir la información a la nube.

Data Transfer Appliance: Envian un dispositivo con mucha capacidad para almacenar datos.

OBJECT STORAGE (ALMACENAMIENTO DE OBJETOS)

Objetos: Imágenes, musica,texto.

Objeto (Metadatos), extensión,duración.

Bucket (Contenedor), donde se va almacenar nuestros objetos.

NameSpace,

Ejemplo:

Nota: El almacenamiento tiene un costo como cualquier otro servicio. Porque los datos o almacenamiento se guardan en una computadora y esa computadora requiere un sistema operativo,almacenamiento interno.

Nota: Importante este concepto

Storage Tier (Niveles de Almacenamiento): Dependiendo de nuestros datos, nosotros vamos a poder definirlo y clasificarlos en 3 diferentes tipos y dependiendo el costo podra ser mayor o menor acorde a las caracteristicas de información.

Acceso Hot- Caliente = Stardard Access

Auto niveles, funciona cuando un archivo u objeto esta siendo manejado/usado con alta o baja frecuencia

OCI OBJECT STORAGE

Es un servicio muy valioso que ofrece Oracle, donde permite realizar diferentes configurciones publicas o privadas y realizar parametrizaciones acorde al tipo de extensión.

BLOCK VOLUME

Consiste en tener una instancia (computadora) y de alguna manera vincularla a nuestro almacenamiento

IOPS – Transferencia de información.

Auto-Tune Performance: Cuando se cambia la instancia, se genera una selección de transferenciade información baja y posteriormente poder conectarlo al almacenamiento anterior.

Los block Volumes pueden ser cifrados.

Bring Your Own Keys: Traer sus propias llaves para tener una comunicación segura.

In transit- Encryption: Los datos que estan en transito instancia y almacenamiento, estan cifrados.

Los block Volumes tienen la capacidad de repartirsen con diferentes maquinas virtuales.Nota: Es bastante utilizado

Podemos iniciar con un block Volume y posteriormente poderlo ir incrementando.

Online—instancia esta conectada con un block volume.

OCI Block Volume

Aca podemos generar nuestro block volume, donde se puede escoger el tipo de transferencia de información.Asi mismo existe la opción de conectarlo con una instancia.

FILE STORAGE (Almacenamiento de Archivos)

En el grafico anterior podemos observar que desde las 2 instancias podran guardar datos al mismo tiempo en el almacnamiento de carpetas.

In Transit TLS ----Es la forma en como se realiza comunicación o como viajan los datos

Se trabaja con sistemas distribuido de archivos

Hipervisores --- diferentes maquinas virtules para realizar la comunicación con el sistema operativo.

Sitios web, repositorios, aplicacionesde oracle,Microservicios y contenedores, escalar aplicaciones y analitica.

BASES DE DATOS

Hay departamentos que se dedidan a la optimización de bases de datos, las BD son fundamentales en cualquier aplicación.

Si falla la BD no se podra consultar información en las aplicaciones.

Bajo desempeño: Tengamos sistemas robustos y rapios al momento de hacer la trasferencia de la información

Latencia Alta: Tiempo en el cual se realiza la consulta de la info y regreso del resultado de busqueda.

Escalabilidad Limitada: Enfocado en los sistemas on-price, necesidad de acuerdo al trafico.

Falta Automatización y seguridad: Tener automatizada ciertas funcionalidades.

Diferentes problemas que podemos tener en el manejo de BD.

Oracle Cloud Public: Cualquier info que se va almacenar en alguna region de oracle.

Customer Data Center: Se puede almacenar cierta info en los servidores.

Depende del tipo de proyecto o empresas, y que hay ciertos requisitos gubernamentales para empresas que necesitan almacenar la info al interior del pais.

Ejemplo: Los bancos, tienen que almacenar la información y no confiarla a proveedores externos.

Base Database Service: Consta en tener una maquina virtual y almacenar mi base de datos.

Exadata Database Service on Dedicate Infraestructure: Un sistema bastante robusto en manejar grandes transferencias de información. Muchos bancos y empesas grandes,utilizan este tipo de servicio.

Autonomous Database on Shared & Dedicated Exadata Infraestructure: Dependiendo de nuestras necesidades y tamaños de los equipos vamos a poder tener ciertas responsabilidades que vamos a realizar, verificación del sistema. Necesitamos mejorar ciertas partes de la BD.

Este sistema autonomo puede ser en una plataforma compartida con diferentes clientes,sin compartir datos.

Servicio en la nube de Exadata.

Depende de las necesidades, el presupuesto y las necesidades del proyecto.

OCI BASE DATABASE SERVICE

La idea es que este servicio pueda ser ejecutado en maquinas virtuales.

Este sistema tiene 2 versiones:

Oracle Enterprise Edition, el cual es destinado para empresas, por la capacidad de almacenamiento y procesamiento.

Nos evitamos la complejidad de realizar una administración manual.

Con unos cuantos click se puede generar una base de datos en OCI.

Enterprise Edition High Performance: La idea es que tenga un desempeño mayor.

Enterprise Edition Extreme Performance: Agregar ciertas capacidades y desempeño ,acorde a las necesidades.

La flexibilidad viene relacionado a las instancias que se requieren, acorde al rendimiento de la bases de datos. Tambien a las necesidad y rendimiento que vaya presentando la base da datos.

Se puede escoger una licencia propia.

La idea es tener una forma en la cual vamos a ejecutar una base de datos en una maquina virtual.

ORACLE AUTONOMOUS DATABASE

Ejemplo de como funciona: Me estoy quedando sin espacio de almacenamiento, va escalarse automaticamente.

Esta fallando, se reinicia y busca las opciones para solucionar.

Ejemplo de Elastica: Quiero que cuando mi BD llegue al 80% me envíe una notificación a mi correo.

ATP: Aplicaciones de transacciones.

ADW: Para análisis de datos, sacar información.

AJD: Optimizado para desarrollo de aplicaciones JSON.

Depende de las necesidades, del tamaño del equipo, depende de factores externos.

ORACLE EXADATA

Es un producto de ORACLE, no necesariamente de OCI.

Servidores/ computadores grandes con mucha capacidad de procesamiento.

Forma de almacenar información, enfocada en procesamientos grandes.

Para aplicaciones pequeñas no necesita tener todaesta infraestructura.

Exadata On-premises: La empresa compra el servidor enfocado en procesamiento y almacenar en las propias instalaciones, adecuación del datacenter en la empresa.

Exadata On-Premise es el modelo de implementación en el que la empresa compra el hardware de Exadata y lo instala en su propio centro de datos. En este caso, la empresa es responsable de la gestión completa de la infraestructura, incluyendo el hardware, el hipervisor, la red, las bases de datos y los datos.

A diferencia de ExaCS y ExaCC, donde Oracle se encarga de la gestión de la infraestructura, en Exadata On-Premise la empresa tiene el control total sobre todos los aspectos del sistema. Esto puede ser una ventaja para algunas organizaciones que tienen requisitos específicos de seguridad, cumplimiento normativo o control de datos.

Sin embargo, también implica una mayor responsabilidad y la necesidad de contar con personal capacitado para gestionar la infraestructura de Exadata.

NW Fabric: Network Fabric --- Se le conoce como la comunicación de mucha intensidad, debe tener baja latencia.

INFINIBAN ------ PREGUNTA DE EXAMEN

NW Fabric: Network Fabric --- Se le conoce como la comunicación de mucha intensidad, debe tener baja latencia entre el DB Servers y Storage Servers.

Esa comunicación de transferencia de datos que va ser super rapida se le conoce cono INFINIBAN.

InfiniBand es una tecnología de interconexión de alta velocidad utilizada en Exadata para proporcionar una comunicación de baja latencia y alto rendimiento entre los servidores de base de datos y los servidores de almacenamiento.

En esencia, InfiniBand actúa como una autopista de datos súper rápida que permite que los componentes de Exadata se comuniquen entre sí de manera eficiente. Esto es crucial para el rendimiento de las bases de datos, ya que permite un acceso rápido a los datos y una transferencia eficiente de la información.

Hypervisor: Un hipervisor es una capa de software que permite la creación y gestión de máquinas virtuales (VMs) en un sistema físico. Piénsalo como un gestor que divide los recursos de un servidor

físico en múltiples entornos virtuales aislados, cada uno funcionando como si fuera una computadora independiente.

En el contexto de Exadata, el hipervisor se encuentra entre el hardware (servidores de base de datos y almacenamiento) y las bases de datos. Permite que múltiples bases de datos operen en el mismo hardware de manera eficiente y aislada.

ExaCS (Exadata Cloud Service)

Recordando en ciertas empresas como bancos, no esta permitido que los datos se almacenen en los servidores de ORACLE.

En este modelo, la infraestructura de Exadata se encuentra en los centros de datos de Oracle Cloud Infrastructure (OCI). Oracle se encarga de la gestión de la infraestructura, incluyendo el hardware, el hipervisor y la red. Tú, como cliente, eres responsable de la gestión de las bases de datos y los datos.

ExaCC (Exadata Cloud at Customer):

En este modelo, la infraestructura de Exadata se instala en tu propio centro de datos, pero es gestionada por Oracle. Oracle se encarga de la gestión de la infraestructura, incluyendo el hardware, el hipervisor y la red, al igual que en ExaCS. Tú, como cliente, sigues siendo responsable de la gestión de las bases de datos y los datos, pero tienes más control sobre la ubicación física de la infraestructura.

En resumen:

ExaCS: Exadata en la nube de Oracle (OCI).

ExaCC: Exadata en tu centro de datos, gestionado por Oracle.

Exadata Autonomous

Autonomous Database en Exadata es la opción donde Oracle se encarga de la gestión de casi todas las capas de la infraestructura y la base de datos. Esto incluye el hardware, el hipervisor, el sistema operativo, el software de la base de datos, la seguridad, las copias de seguridad y la recuperación. Como cliente, solo eres responsable de cargar tus datos y definir la estructura de la información.

En esencia, Autonomous Database automatiza muchas de las tareas de administración de la base de datos, lo que te permite concentrarte en el desarrollo de aplicaciones y el análisis de datos.

MYSQL HEATWAVEWAVE

HearWave: Es un acelerador de consultas en memoria. Dentro de este concepto se integra el aprendizaje automatico (Machine Learning).

MySQL es mucho mas economico que otras consultas en la nube como Aurora de AWS.

NoSQL DATABASE (No Only SQL)

MongoDB es un ejemplo de bases de datos NoSQL.

Se ejecutan en la nubo.

SQL ---- Diseño de formato tabla.

NoSQL---- key – value (JSON) Es la forma en como se realiza la transferencia de información entre sistemas.

Column –Family: Tiene mas flexibilidd al momento de almacenar la información.

Graph – Almacenamiento mas avanzado, requiere matematicas.

CREANDO UNA DB EN OCI

SEGURIDAD

Trata de toda la seguridad de la infraestructura OCI.

Modelo de Seguridad Compartida

on-premise" se refiere a los sistemas donde la empresa gestiona toda la infraestructura, incluyendo servidores, almacenamiento de datos, dispositivos, cuentas de usuario, aplicaciones, redes, sistemas operativos, virtualización, red física y centros de datos. En este modelo, la empresa es totalmente responsable de la seguridad y el mantenimiento de toda la infraestructura.

MFA: significa "Multi-Factor Authentication" (Autenticación Multi-Factor). Es una capa adicional de seguridad que se añade al proceso de inicio de sesión. En lugar de depender únicamente de una contraseña, el MFA requiere que el usuario proporcione dos o más factores de verificación para acceder a una cuenta o aplicación.

La "Protección contra DDoS" es un conjunto de técnicas y servicios diseñados para mitigar y prevenir los ataques de Denegación de Servicio Distribuida (DDoS). El objetivo principal de esta protección es asegurar que un servicio en línea (como un sitio web, una aplicación o una red) permanezca disponible y funcional incluso durante un ataque DDoS.

En el contexto de la clase, la protección contra DDoS se menciona como un servicio de seguridad que protege la infraestructura, específicamente las redes y los servidores, evitando que colapsen debido a un exceso de peticiones.

---------//----------

En el contexto de la clase, "OS and Workload Protection" se refiere a la protección de los sistemas operativos y las cargas de trabajo que se ejecutan en los servidores. Esto incluye tanto el sistema operativo en sí como las aplicaciones y los datos que se procesan en él.

Para proteger los sistemas operativos y las cargas de trabajo, se utilizan varias técnicas y servicios, como:

Shield Instances: Instancias seguras diseñadas para garantizar un inicio seguro siguiendo ciertas reglas y utilizando sistemas operativos e imágenes seguras.

Dedicated Host: Servidores exclusivos para un solo cliente, lo que añade una capa extra de seguridad al no compartir el hardware con otros usuarios.

Sistemas Operativos Seguros: Sistemas operativos que se actualizan constantemente con mejoras de seguridad.

Bastión: Aunque no se entra en detalle en la clase, Bastión es un servicio que proporciona acceso seguro a las instancias en la nube, evitando la exposición directa a Internet.

----------//----------

Data Protection

En el contexto de la clase, "Data Protection" (Protección de Datos) se refiere a cómo almacenamos de forma segura nuestra información en instancias, buckets o sistemas, y cómo aseguramos el envío de información a través de aplicaciones. Esencialmente, se trata de proteger la confidencialidad, integridad y disponibilidad de los datos.

Algunos de los servicios y conceptos clave relacionados con la protección de datos en OCI son:

Vault: Actúa como una "caja fuerte" para información sensible. Incluye:

Vault Key Management: Gestión de claves de cifrado para proteger los datos.

Vault Secrets Management: Gestión de secretos, como contraseñas, tokens y certificados.

Certificates Authority: Proporciona seguridad adicional al trabajar con datos, gestionando certificados digitales.

Es importante recordar que, como empresa o persona, somos responsables de la seguridad de los datos, no solo OCI. Esto significa que debemos implementar medidas de seguridad adecuadas para proteger nuestros datos, como el cifrado, el control de acceso y la gestión de claves.

----------//----------

Detection and Remediation

En el contexto de la clase, "Detection and Remediation" (Detección y Remediación) se refiere al proceso de identificar y corregir errores, vulnerabilidades o intrusiones en la infraestructura de la nube. Este proceso es crucial para mantener la seguridad y la integridad de los recursos en OCI.

El servicio principal que se menciona en la clase para la detección y remediación es Cloud Guard. Este servicio actúa como un "guardia de la nube", vigilando los recursos y notificando intrusiones o cambios de política. Cloud Guard puede:

Enviar notificaciones a grupos específicos cuando se detectan problemas.

Corregir errores automáticamente, dependiendo de la configuración.

Realizar escaneo de vulnerabilidades para identificar posibles puntos débiles en la seguridad.

Ayudar en el manejo de amenazas, proporcionando información y herramientas para responder a incidentes de seguridad.

TERMINOS IMPORTANTES PARA LA CERTIFICACIÓN – SEGURIDAD

Cloud Guard

Vault Key Management

Vault Secret Management

IAM (Identity and Access Maganement)

Creando Security Zone

Nota: Para generar la zona de seguridad, primero se debe activar el cloud guard.

CLOUD GUARD

Cloud Guard es un servicio dentro de Oracle Cloud Infrastructure (OCI) diseñado para ayudarte a detectar problemas, verificar configuraciones y monitorear la actividad de tu infraestructura en la nube.

Aquí hay algunos puntos clave sobre Cloud Guard:

Objetivo (Target): Son los elementos o recursos que deseas monitorear, como instancias (máquinas virtuales), buckets (contenedores de almacenamiento) o direcciones IP.

Detectores (Detectors): Identifican posibles errores o problemas. Por ejemplo, un detector puede activarse si una instancia o un bucket se vuelve público.

Problemas: Son los problemas de seguridad identificados por los detectores.

Respondedores (Responders): Definen las acciones a tomar cuando se detecta un problema. Por ejemplo, detener automáticamente una instancia que se ha vuelto pública o deshabilitar un bucket que se ha hecho público.

Un bucket público es un contenedor de almacenamiento en la nube que está configurado para permitir el acceso a cualquier persona en Internet, sin necesidad de autenticación.

Imagina que tienes un armario donde guardas tus archivos. Normalmente, solo tú tienes la llave para acceder a él. Pero si conviertes ese armario en un "bucket público", sería como dejar la puerta abierta para que cualquiera pueda entrar y ver lo que hay dentro.

En el contexto de la nube, esto significa que cualquier persona podría ver, descargar o incluso modificar los archivos almacenados en ese bucket, dependiendo de los permisos configurados.

SECURITY ZONE AND SECURITY ADVISOR

(Zona de seguridad y Agente de seguridad)

Una Security Zone es un compartimento en Oracle Cloud Infrastructure (OCI) donde puedes incluir recursos como instancias, redes virtuales en la nube (VCNs) y bases de datos, con la característica clave de que la seguridad no se puede deshabilitar.

Piénsalo como una "caja fuerte" para tus recursos en la nube, donde aplicas reglas de seguridad (llamadas Security Zone Recipes) que determinan qué acciones están permitidas. Por ejemplo, puedes establecer una regla para que todas las subredes en ese compartimento sean privadas, impidiendo la creación de subredes públicas.

El Security Advisor es un servicio en la nube que unifica las Security Zones, Cloud Guard y otras capacidades de seguridad de OCI. Actúa como un agente que te ayuda a mantener la seguridad en diferentes servicios, como Object Storage Buckets, File Systems, Virtual Machine Instances y Block Volumes.

Este agente tiene reglas predefinidas que te ayudan a crear estos elementos con una capa de seguridad adicional. Por ejemplo, puedes usarlo para asegurar que la mayoría de tus Buckets sean privados o para aplicar un cierto nivel de seguridad a tus máquinas virtuales.

Podemos observar que dentrode una región podríamostener compartimientos con zonasde seguridad y otros sin zona de seguridad.

Donde se establecen reglas o recetas,asi mismo al momento de integrar recursos en el compartimiento con zona de seguridad, van a existir reglas o politicas que se deben cumplir.

Ejemplo:

Solo se permite crear redes privadas. Si quieres crear una red publica no te va permitir realizarlo. Entre otras cosas.

Nos va ayudar tener cierta seguridad en los diferentes serivicios mencionados en la imagen.

Ya tiene reglas establecidas para generar diferentes tipos de elementos, con una CAPA de seguridad. Prima la privacidad.

ENCRYPTION – CIFRADO

el concepto de encryption (cifrado) como una forma de convertir texto en una serie de caracteres que representan la misma información, pero de manera cifrada. Hablamos sobre cómo este proceso agrega una capa de seguridad, requiriendo un algoritmo para descifrar el texto y obtener la información comprensible.

También cubrimos los tipos de cifrado, como encryption at rest (cuando los datos están almacenados) y encryption in transit (cuando los datos se transmiten de forma segura).

Además, comparamos el cifrado simétrico (que utiliza una sola llave para encriptar y descifrar) con el cifrado asimétrico (que utiliza dos llaves: una pública para encriptar y una privada para descifrar).

El cifrado simétrico es el método más sencillo de encriptación, ya que utiliza la misma llave tanto para encriptar como para desencriptar la información.

Imagina que tienes un diario personal y quieres asegurarte de que nadie más pueda leerlo. Con el cifrado simétrico, utilizas una llave secreta (como una palabra clave o una frase) para bloquear el diario. Cuando quieres leerlo, usas la misma llave para desbloquearlo.

La ventaja principal del cifrado simétrico es su velocidad y eficiencia, lo que lo hace ideal para encriptar grandes cantidades de datos. Sin embargo, su principal desventaja es que la seguridad depende de mantener la llave secreta a salvo. Si alguien más obtiene acceso a la llave, podrá leer toda la información encriptada.

El cifrado asimétrico es un poco más complejo que el simétrico, pero ofrece una mayor seguridad. En lugar de usar una sola llave, utiliza dos llaves diferentes:

Llave pública: Se utiliza para encriptar la información. Puedes compartir esta llave con cualquier persona.

Llave privada: Se utiliza para desencriptar la información. Debes mantener esta llave en secreto y no compartirla con nadie.

Imagina que quieres recibir un mensaje secreto de un amigo. Le das tu llave pública, y él la utiliza para encriptar el mensaje antes de enviártelo. Una vez que recibes el mensaje encriptado, utilizas tu llave privada para desencriptarlo y leerlo.

La principal ventaja del cifrado asimétrico es que no necesitas compartir tu llave privada con nadie, lo que reduce el riesgo de que alguien la intercepte. Sin embargo, es más lento y requiere más recursos computacionales que el cifrado simétrico.

Un Hardware Security Module (HSM) es un dispositivo físico diseñado para proteger y administrar claves criptográficas. Piénsalo como una caja fuerte digital para tus llaves más importantes.

En lugar de almacenar las claves en un software, donde podrían ser vulnerables a ataques, el HSM las almacena en un hardware seguro y resistente a la manipulación. Esto proporciona una capa adicional de seguridad, ya que los atacantes tendrían que acceder físicamente al HSM para robar las claves.

Los HSM se utilizan en una amplia variedad de aplicaciones, como la banca en línea, el comercio electrónico y la infraestructura de clave pública (PKI). Oracle Cloud Infrastructure (OCI) utiliza HSM en su servicio Vault para proteger las claves de cifrado de los clientes.

VAULT

exploramos el concepto de Vault como una herramienta centralizada para manejar llaves y credenciales de manera segura.

Vault te permite almacenar tanto llaves, que son esenciales para el cifrado y descifrado de datos, como "secrets", que pueden ser contraseñas, certificados, llaves SSH o tokens de autenticación. Esencialmente, actúa como un almacén seguro para datos sensibles, protegiéndolos de accesos no autorizados.

Entiendo tu interés en las llaves maestras de seguridad protegidas por software dentro de Vault.

En Vault, tienes la opción de proteger tu llave maestra de dos maneras: mediante software o mediante un HSM (Hardware Security Module). Cuando eliges la protección por software, los datos se almacenan en el servidor y pueden ser exportados desde allí. Esta opción es más flexible y generalmente gratuita, pero puede ser menos segura que usar un HSM.

La llave maestra es crucial porque se utiliza para cifrar y descifrar la información almacenada en tu Vault. Además, puedes auditar el uso de la llave maestra, registrando cuándo y quién la utilizó.

----------//----------

Cuando eliges proteger tu llave maestra con un HSM, estás utilizando un dispositivo de hardware específico diseñado para almacenar datos sensibles de manera segura. A diferencia de la protección

por software, los datos almacenados en un HSM no pueden ser exportados, lo que proporciona una capa adicional de seguridad. Sin embargo, esta opción generalmente tiene un costo asociado.

La "Master Key" o llave maestra es un componente central en el funcionamiento de Vault.

En esencia, la llave maestra es la llave principal que se utiliza para cifrar y descifrar todas las demás llaves y secretos almacenados en tu Vault. Piénsalo como la llave que abre la puerta a todas las demás llaves.

Es crucial proteger la llave maestra, ya que si se pierde o se ve comprometida, podrías perder acceso a toda la información almacenada en tu Vault. Por eso, Vault ofrece opciones para proteger la llave maestra mediante software o mediante un HSM (Hardware Security Module), como mencionamos antes.

Además, Vault te permite auditar el uso de la llave maestra, lo que significa que puedes registrar cuándo y quién la utilizó. Esto te ayuda a mantener un control sobre quién tiene acceso a la llave maestra y cómo se está utilizando.

El "Envelope Encryption" (cifrado de sobre) es una técnica de cifrado que se utiliza para proteger datos sensibles mediante el uso de múltiples capas de cifrado.

En esencia, el Envelope Encryption funciona de la siguiente manera:

Cifrado de los datos: Primero, los datos se cifran con una clave de datos (data key). Esta clave de datos se genera aleatoriamente y se utiliza solo para cifrar los datos específicos.

Cifrado de la clave de datos: Luego, la clave de datos se cifra con una clave de cifrado de claves (key encryption key o KEK). Esta KEK es una clave que se almacena y gestiona de forma segura en un sistema de gestión de claves, como Vault.

Almacenamiento de los datos cifrados y la clave de datos cifrada: Finalmente, los datos cifrados y la clave de datos cifrada se almacenan juntos.

Para descifrar los datos, se sigue el proceso inverso:

Descifrado de la clave de datos: Primero, la clave de datos cifrada se descifra con la KEK almacenada en el sistema de gestión de claves.

Descifrado de los datos: Luego, la clave de datos descifrada se utiliza para descifrar los datos cifrados.

NOTA: Si pierdes tu Master Key, no vas a poder recuperar la información incriptada. Ni si quiera Oracle podra ayudarnos.

En la imagen anterior se puede ver un flujo usando el recurso Vault para incriptar un objeto (documento) y la asignación de llaves y llave maestra, asi como la desincriptación.

COMO ACCEDER A VAULT

Nota: Para la generación de Vault en OCI requiere cierto tiempo.

GOBERNANZA Y ADMINISTRACIÓN

Precios

Los servicios que frece OCI son los de menor que ofrece el servicio de nubo que actualmente existen en el marcad.

En esta lección, exploramos los modelos de precios en Oracle Cloud Infrastructure (OCI), incluyendo el modelo de pago por uso, los créditos universales anuales y la opción de traer tu propia licencia. También analizamos los factores que influyen en el precio, como el tamaño de los recursos, la transferencia de datos y el tipo de recurso utilizado.

El modelo pay-as-you-go (PAYG) es ideal para quienes están dando sus primeros pasos en la nube, ya que solo se cobra por los recursos utilizados. Por ejemplo, si creamos una instancia para realizar un ejercicio o un ejemplo de un tutorial, la generamos y la destruimos al terminar el ejercicio. Si nos lleva uno o dos días, solo se cobrará por ese tiempo de uso. No hay compromiso inicial ni un periodo de servicio mínimo, por lo que podemos utilizar una hora, dos horas, un día o una semana, dependiendo de nuestras necesidades. Al final, se cobra por la utilización medida por hora. Este modelo se basa en el consumo para servicios como Oracle Functions, instancias o computadoras, ya sean virtual machines o bare metal machines.

----------//----------

Los Annual Universal Credits (créditos universales anuales) implican comprometerse a comprar créditos que se utilizarán según tus necesidades en diferentes servicios de OCI, como instancias, almacenamiento o bases de datos. Este modelo ofrece ahorros significativos y funciona de manera similar a las membresías de gimnasio o plataformas de streaming, donde compras acceso por un año y obtienes un descuento en lugar de pagar mes a mes.

Es importante tener en cuenta que, al final del año, los créditos no utilizados no son reembolsables, por lo que deben ser utilizados sí o sí. Además, hay descuentos basados en el tamaño y los términos del acuerdo. Por ejemplo, si compras créditos para un gran número de instancias, los descuentos por volumen pueden ser considerables.

El modelo Bring Your Own License (BYOL) permite a las empresas o personas que ya poseen licencias de bases de datos o software específico reutilizarlas en OCI. Esto facilita la migración a la nube al permitirte aprovechar las licencias existentes en lugar de tener que adquirir nuevas.

Cuando un usuario entra a una aplicación a visualizar información como datos,videos,entre otras cosas OCI, comienza a cuantificar el uso de esos recursos. Adicionalmente cuando quieremos enviar o trasferir información entre regiones tendra un costo.

Si la transferencia de información se realiza en el mismo dominio de disponibilidad no tendra costos asociados.

MANEJO DE COSTOS

Budgets(Presupuestos)

En Oracle Cloud Infrastructure (OCI), la funcionalidad de "budgets" (presupuestos) te permite crear un presupuesto específico para monitorear cuánto se ha gastado y consumido en recursos. Por ejemplo, puedes crear un presupuesto llamado DepTest asignándole un monto de $1,000.

Al establecer este presupuesto, puedes monitorear cuánto se ha gastado en el mes y cuánto has consumido en recursos. Esto te ayudará a configurar alertas que lleguen a tu correo electrónico para saber cuándo estás próximo a completar un presupuesto.

El "Cost Analysis" (análisis de costos) es una herramienta que te permite realizar consultas de tu histórico de gastos, ya sea diario, semanal o por fecha, y agregar filtros. Por ejemplo, puedes consultar cuánto has gastado en instancias de alguna zona de disponibilidad o región.

Al realizar un análisis de costos, puedes agregar filtros y ver en detalle cuáles son los días con mayor impacto en el costo. Puedes comparar el costo contra la fecha y ver los diferentes servicios y su impacto en el costo. Por ejemplo, si la mayoría del costo proviene del servicio de Compute, ya sea por instancias, máquinas virtuales, puedes identificarlo visualmente.

Los "usage reports" (reportes de uso) te permiten generar reportes diarios que se exportan en formato CSV. Estos archivos CSV pueden ser utilizados para graficar o integrarlos en sistemas externos, como Power BI, Tableau o cualquier plataforma que la empresa utilice y que pueda leer este tipo de archivos.

Estos reportes pueden ser útiles para generar informes de uso, permitiendo que el equipo de administración de TI o tu propio equipo monitoree los costos asociados a cada proyecto en el que están involucrados o a todos los proyectos de la empresa.

Las cuotas te permiten establecer cuántos servicios se pueden tener, dependiendo de un compartimento específico, y fijar un límite. Por ejemplo, si tienes una máquina virtual o instancia estándar 2.1, puedes limitar su uso a 100 instancias.

En cuanto a las cuotas de compartimento, tenemos tres escenarios:

Set (configurar): Estableces el número máximo de recursos que un compartimento puede usar. Por ejemplo, el máximo es 100.

Unset (restablecer): Restablece las cuotas a un límite por defecto para cada servicio.

Zero (eliminar): Elimina el acceso a recursos del compartimento, útil si quieres restringir el acceso a un compartimento específico.

CLOUD ADVISOR

TAGGING (ETIQUETADO)

El tagging o etiquetado es un concepto clave en la gestión de recursos en la nube. Se refiere a la posibilidad de añadir etiquetas a recursos como instancias, buckets, redes y partes de almacenamiento. Estas etiquetas son pares de clave-valor que ayudan a organizar y buscar recursos de manera más eficiente.

Por ejemplo, puedes tener una etiqueta con la clave "proyecto" y el valor "frontend", lo que te permite identificar rápidamente a qué proyecto pertenece un recurso específico. Además, las etiquetas pueden ser útiles para gestionar costos, ya que puedes crear presupuestos basados en ellas.