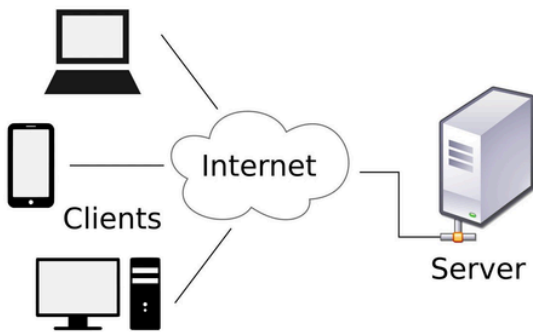


Amazon Web Services

Cloud Practitioner



Cloud Computing



El modelo cliente-servidor es un modelo que nos ayuda a saber el funcionamiento de una aplicaciones, donde los clientes hacen uso de servicios proporcionados por el servidor, ya sea gestión de datos, base de datos o almacenamiento

On-Premise (IT Tradicional)

El modelo On-Premise hace referencia a cuando la compañía tiene sus propios servidores en un lugar y ellos se encargan al 100% de mantenimiento de sus servidores, OS, almacenamiento, funcionalidad, etc.

- Pago de electricidad, refrigeración, etc.
- No es escalable.
- Añadir software y sustituir cuando es necesario.
- Posibles catástrofes.
- Supervisar un equipo 24 horas.



CLOUD



ON-PREMISE

Cloud Computing

Con el Cloud Computing los problemas de mantenimiento, OS y persistencia del servidor se encargara una empresa externa, como AWS, los servidores ya no los compras y los tienes en tu oficina, si no que Amazon te los renta por ello.

- Plataforma de servicios de servidores pagando solo por lo que se usa.
- Puedes poner características al servidor que tu quieras
- Acceso a recursos tanto como necesites al instante
- Forma fácil de acceder a servidores, almacenamiento, bases de datos, servicios



Ventajas del Cloud Computing

- Cambia el gasto de capital por gasto operativo (Rentar / no comprar)
- Te beneficias de economías de escalas masivas
- Deja de adivinar la capacidad de servidores que ocupas
- Aumentar velocidad y agilidad
- No gastas en mantenimiento de servidores
- Puedes ser global gracias a la escalabilidad

Amazon Web Services

Cloud Practitioner



Modelos de Cloud

- *Privado*: No expuestos al público, satisface necesidades empresariales específicas.
- *Público*: Controlada por proveedor de servicios (AWS, Azure, Google Cloud).
- *Híbrido*: Puedes tener servidores tanto en tu oficina como en AWS, aprovechando el potencial de ambos.

Características de Cloud con AWS

- Autoservicio (Usas el sistema de AWS para administrar).
- Acceso por red (Internet).
- Alquiler múltiple: Varios clientes pueden compartir servicios y aplicaciones de forma segura.
- Elasticidad en escalabilidad: Crece y decrece el poder del servidor cuando quieras.
- Se paga solo por lo que se usa.
- Alta disponibilidad de los servidores rentados (Si hay catástrofe AWS se encarga de tus datos).

Tipos de Cloud Computing

IaaS (Infraestructura como servicio)

Se renta una infraestructura virtualizada de un servidor.
Ejemplo: EC2.

Paas (Plataforma como servicio)

Ofrece una plataforma donde se pueden desarrollar aplicaciones sin preocuparse por la infraestructura, solo por la aplicación a desarrollar.
Ejemplo: Elastic Beanstalk de AWS.

SaaS (Software como servicio)

El proveedor ofrece tanto la infraestructura y la aplicación, por lo que el usuario final no usa ningún tipo de recurso en su monitor, todo se ejecuta en la nube.
Ejemplo: Zoom, Drive.

Tipos de cobros en AWS.

- Por computación o tiempo de uso (Lambda AWS)
- Por Almacenamiento (S3 Amazon)
- Por transferencia de datos FUERA de Cloud (Interna es gratuita en AWS)

Infraestructura Global



Regiones

Se tienen regiones o instalaciones en todo el mundo, estas regiones tienen o pueden no tener algunos servicios, cada región se divide en zonas de disponibilidad (AZ), cada región está aislada de las demás (us-east-1).
Oregón, Sydney, Tokio

Zonas de Disponibilidad (AZ)

Ubicadas en las regiones, son varias instalaciones físicas comunicadas en una red de baja latencia, separadas entre sí.
us-east-1a, us-east-1b

Centros de Datos

Una zona de disponibilidad puede tener uno o varios centros de datos, administrados por AWS para ser altamente disponibles.

Puntos de presencia

Amazon Web Services

Cloud Practitioner



Como elegir la AZ y la región

- Cumplimiento de requisitos legales y gobernanza de datos.
- Proximidad de clientes (que este cerca).
- Servicios disponibles de la región.
- Precios (Los precios son diferentes en cada región).

Tipos de Servicios

Servicios que funcionan globalmente.

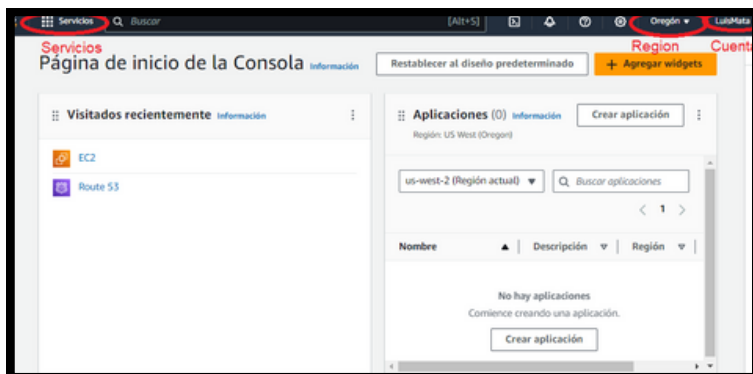
- IAM.
- Route 53 (Servicio DNS).
- CloudFront.
- WAF (Firewall de aplicaciones web).

Servicios que funcionan por región

- EC2 (IaaS).
- Elastic Beanstalk (PaaS).
- Lambda (Función como servicio).
- Rekognition (SaaS).
- Etc...

<https://aws.amazon.com/es/about-aws/global-infrastructure/>

Consola



Responsabilidad Compartida.



<https://aws.amazon.com/es/compliance/shared-responsibility-model/>

IAM

Identity and Access Management (GLOBAL)

Crea grupos de usuarios para que no uses la cuenta root, y así, cada usuario pueda hacer y no hacer lo que le indiques en la política.

- Los usuarios pueden estar en 0 o N cantidad de grupos de políticas.
- Cada grupo tiene sus restricciones de accesos.
- Un usuario puede tener su política propia sin estar en algún grupo.

Estructura del JSON de una política.

Version: versión del lenguaje de la política.

Id: un identificador para la política (opcional)

Statement: una o más declaraciones individuales (obligatorio)

Sid: un identificador para la declaración (opcional)

Effect: si la sentencia permite o deniega el acceso (Permitir, Denegar)

Principal: cuenta/usuario/rol al que se aplica esta política.

Action: lista de acciones que esta política permite o deniega

Resource: lista de recursos a los que se aplican las acciones

Amazon Web Services

Cloud Practitioner



Ejemplo JSON de politica.

```
{
  "Version": "2012-10-17",
  "Id": "S3-Account-Permissions",
  "Statement": [
    {
      "Sid": "1",
      "Effect": "Allow",
      "Principal": {
        "AWS": ["arn:aws:iam::123456789012:root"]
      },
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": ["arn:aws:s3:::mybucket/*"]
    }
  ]
}
```

Una politica define un conjunto de permisos para acciones en uno o varios servicios, estas politicas se pueden asignar a grupos o usuarios, hay unas ya hechas y puedes personalizarlas tambien.

Multi Factor Authentication

Si a un morro lo hackean su cuenta root o IAM, van a tirar todo en segundos, MFA permite que aparte de la contraseña, agregues un dispositivo de seguridad, con el que identificas el token de acceso.

Opciones

- Dispositivo MFA (Google autenticador o authy)
- U2F
- Llaverio MFA

Para configurar una politica de contraseña has de ir a IAM > configuracion de la cuenta
Para configurar un MFA has de ir a perfil > credenciales de seguridad

Formas de acceder a AWS

- Por consola de administracion. (MFA/ contraseña)
- Por linea de comandos CLI. (claves acceso)
- Por SDK (claves de acceso)

Id de la clave de acceso => usuarios

Clave de acceso => contraseña

(Cada usuario administra sus claves de acceso)

AWS cloudshell

Servicio para usar AWS cli desde el navegador, asi ya no importa tu sistema operativo o tener que instalarlo.

Un rol de IAM tambien puede asignarse a servicios

Reportes de IAM

IAM credentials report -> Muestra los reportes de todos los usuarios.

IAM Access Advisor -> Reporte de un usuario en concreto.

AWS Budget

Permite ponerle un maximo de gasto a todo lo que uses en AWS, maximo de dinero en general o ser especifico en cuanto quieres gastar en cada servicio.

EC2

EC2 (Elastic Cloud Computing) es un servicio de renta de computo virtual de servicorees, a cada de estas maquinas las conoceremos como instancias.

- Alquilar maquinas virtuales.
- Almacenar datos en unidades virtuales.
- Distribuir cargas
- Escalar los servicios con ASG (Auto-Scaling Group)

Tu personalizas

- Sistema operativo
- Memoria de Almacenamiento (EBS y EFS)
- RAM
- Tarjeta de red
- Grupo de seguridad (Que entra y sale de)

Bootstrapping: Comandos que se ejecutaran al crear la instancia.

AMI (Amazon Machine Image)

Al igual que en Docker, es la base de una computadora que define los componentes de software que tendra la maquina.

Amazon Web Services

Cloud Practitioner



Para acceder a la instancia EC2 generaras un archivo .pem o .ppk para Putty, dependiendo que sistema operativo use tu maquina para conectarte por SSH a la instancia.

Si apagas y prendes la instancia es posible que la IP publica de la instancia cambie.

Tipos de clase de instancias

- General
- Computed optimized
- Memory optimized
- Accelerated computing
- Storage optimized
- Instance features
- Measuring instance

m5.2xlarge

m = Clase de la instancia

5 = Generacion

2xlarge = Tamaño de la instancia

Grupos de seguridad.

Un grupo de seguridad puede controlar la entradas y salidas de una o mas instancias, donde le colocas el protocolo, el puerto y la ip autorizada.

Tipos de compra.

- Bajo demanda (Pagas por tiempo de uso, sin compromiso).
- Reservadas (Reservas de 1 o 3 años de uso, con buen descuento). hay convertibles (cambiar recursos) y las que no.
- Instancias Spot (Las mas baratas, pero por subastas, si alguien paga mas te vas).
- Host dedicado (Compras todo el edificio)
- Reserva de capacidad (Reservas lo que quieres sin importar si lo usas o no lo pagas)
- Planes de ahorro (Como un buffet, pagas algo bueno pero usas lo que quieras)

EBS Elastic Block Store

Es para hacer que las instancias tengan almacenamiento persistente, pues si terminas la instancia todo en ella pierde la informacion, mediante un dispositivo en red.

Un EBS solo se puede conectar a una instancia, pero una instancia a uno o mas EBS.

Un EBS no se comunicara con instancias que esten en otra zona de disponibilidad

Snapshots (Instantaneas)

Es un respaldo para las EBS, lo puedes usar para sacarle respaldo, tambien para mover un EBS de una AZ a otra.

Sacas una copia de un EBS en una Snapshot y lo copias en otra EBS que este en otra AZ.

Si una snapshot se convierte en un archivo sale mas barato.

Papeleria de reciclaje para snapshots

Existe una papeleria donde puedes definir los numeros de dias de tolerancia antes de que se elimine la snapshot.

AMI y EC2 image builder

Igual que docker es una imagen de una maquina virtual para facilitar el proceso de tener componentes de software en la maquina.

Se contruyen por region pero puedes copear y pegar.

Tipos de AMIs:

- AMI publica (propias de AWS)
- AMI propia (La creas tu)
- AMI marketplace (La compras a otros)

EC2 image builder

Servicio que automatiza la creacion de imagenes.

Crea una imagen con una instancia a EC2 con la receta que le digas, luego al tener la AMI la usa en otra EC2 para ver si jala chido y al final de esto ya tienes la AMI para distribuir

A estre proceso de EC2 image builder se llama pipeline y la puedes programar para que se haga cada cierto tiempo.

Amazon Web Services

Cloud Practitioner



Elastic Load Balance

2 tipos de escalabilidad:

- **Vertical:** Aumentar el tamaño de una instancia t2.micro -> t2.large.
- **Horizontal** (elasticidad): Aumentar el numero de instancias. (sistemas distribuidos)

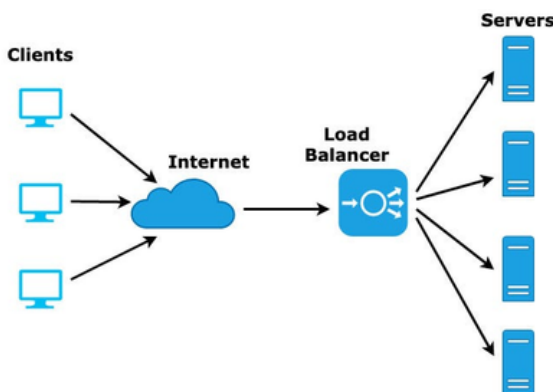
Alta disponibilidad (Ejecutar un sistema en al menos 2 zonas de disponibilidad) Evitar que si se muere el centro de datos muera toda tu app, puesto que tambien la tienes en otro lado.

Elasticidad: Aumentar dependiendo de la carga de forma automatica (crecer y decrecer)

Agilidad: Hacer todo a un solo click

Load balancing (En horizontal)

Se encarga de distribuir las peticiones de los distintos clientes a distintos servidores para que no caiga siempre al mismo y lo mates. Y solo expone un DNS, si muere una instancia el load balancer detecta y no envia la peticion ahi.



Balancer HTTP - Capa 7 DNS

Network balancer - Capa 4 IP estatica

Gateway balancer - Capa 3 Detecciona intruso

Classic Balancer - Capa 4 y 7 (en desuso)

Auto Scaling Group

Reducir y aumentar instancias EC2 para que coincida con la carga y asegurarse de un numero minimo y maximo de instancias.

Se crean instancias automaticamente y se agregan automaticamente al load balancer.

Escalado manual: Tu actualizas el ASG manual
Escalado Dinamico:

- Simple: AWS CloudWatch te avisa cuando se añaden unidades y cuando se quitan en base a el uso de las instancias
- Seguimiento: Decir cuanta capacidad es la que quieres en promedio para cada instancia
- Programado: Anticipar un patron de usos de las instancias para tener mas o menos
- Predictivo: El machine learnig lo decide con antelacion

S3

Servicio de almacenamiento de AWS, para guardar aplicaciones, medios, recuperacion de desastres, copias de seguridad o sitios estaticos.

Cada **bucket** permite almacenamiento de archivos, debe tener nombre unico global y es a nivel de region, a pesar de ser global.

Objetos (archivos) guardados en s3 tienen una clave y tiene una ruta completa (pelicula, archivos, etc) y guarda maximo 5 teras un objeto y puede tener ID o etiquetas.

Seguridad en los buckets

- Basada en usuarios IAM.
- Basada en politicas de buckets y lista de control de acceso

Versionamiento en buckets

Cada objeto en un bucket puede tener versionamiento como en GIT para volver a su version anterior

Amazon Web Services

Cloud Practitioner



Replicar info de un bucket a otro.

Para copiar la info de un bucket a otro debe de:

- Ambos buckets tener activado el versionamiento.
- Replicación entre regiones (CRR).
- Replicación entre la misma región (SRR)
- Los buckets pueden no estar en la misma cuenta y funcionará.
- Debe de tener permisos para hacer esto y ser asíncrono.

Para lograrlo se crean reglas de replicación diciendo origen y destino.

Clases de almacenamiento.

- Standard (para apps o big data).
- Standard Infrequent Access (Copias de seguridad).
- One zone Infrequent Access (Copias de seguridad secundaria, en una AZ).
- Glacier Instant Retrieval (Pagas poco por guardar pero pagas para recuperar, es rápido).
- Glacier Flexible Retrieval (Tardas más en recuperar la info).
- Glacier Deep Archive (Tarda 12/48 horas en recuperar).
- Intelligent Tiering (Con machine learning decide que tipo de clase es mejor).

Durabilidad: No pierdes los datos.

Disponibilidad: Puedes recuperarlos cuando quieras (disponible el servicio S3 siempre)

Reglas de ciclo de vida: Le dices a un objeto o varios, a durante 30 días estás en standard y luego 2 años en glacier y así.

S3 OBJECT BLOCK Y GLACIER VAULT

WORM => Write once, read many.

S3 object Block: Bloquear que no se pueda borrar objetos.

Glacier Vault: Que las políticas no se puedan cambiar.

Cifrado en S3

AWS cifra en su lado de backend cuando le subes un archivo a un bucket, pero también si quieres más seguridad, puedes subirlo tú ya cifrado desde el cliente.

AWS Snow family

Dispositivos de alta seguridad para recopilar, procesar y migrar datos a AWS (sin conexión)

Migración de datos:

- Snowcone (Resiste climas chidos 8Tb y 14Tb, más chico que edge)
- Snowball Edge (Para transferir archivos 80Tb y 42Tb)
- Snowmobile (Hasta 1 millón de Tb, es un pinche camión alv wtff).

Edge computing:

- SnowCone
- Snowball Edge

Dispositivos físicos para subir archivos pesados sin internet a AWS (S3 por ejemplo) para que no lo hagas desde la web. El dispositivo te llega y lo mandas a AWS físicamente.

Solicitas el snow desde AWS, instalas el cliente Snowball, te llega el dispositivo, le metes la info y lo devuelves.

AWS OpsHub

Te ayuda a configurar de forma fácil un snow, ver cuánto has usado y hasta puedes controlar y lanzar servicios de AWS.



Storage gateway

Para hacer cloud híbrido, para hacer que tus servidores puedan usar AWS, puedes tener respaldo de tus ficheros en AWS o en físico, como desees.

Servicios para bases de datos

RDS (Relational Database Service)

Servicio especializado para bases de datos relacionales con SQL como MySQL, SQL, MariaDB, etc. Ofrece como versionamiento, copias de seguridad, y el OS para eso.

Amazon Web Services

Cloud Practitioner



Amazon Aurora

Optimizado para SQL en Amazon y mejor que RDS, útil para PostgreSQL y MySQL, es más caro, pero escala el almacenamiento automáticamente.

Amazon ElastiCache

Para bases de datos basadas en memoria (cache) como Redis o Memcached

DynamoDB

Para bases de datos no relacionales (NoSQL) y ayuda a almacenar cientos de TB, es autoescalable. Para bases de datos clave-valor. Puedes usar DynamoDB Accelerator (DAX) para mejorar el rendimiento (serverless).

RedShift

Se basa en PostgreSQL pero no usa OLTP, carga datos cada hora y no por segundo (Para análisis y almacenamiento de datos) y tiene 10 veces mejor rendimiento que otros servicios para BD ALMACEN DE DATOS.

Amazon EMR (Elastic Map Reduce)

Elastic MapReduce, servicio útil para el *análisis de datos*, clusters, (big data), procesar gran cantidad de datos y autoescalable.

Amazon Athena

Para analizar datos almacenados en S3 sin servidor, utiliza SQL y admite JSON, CSV, ORC.

Amazon QuickSight

Para crear dashboards para análisis empresariales con Machine Learning sin servidor.

DocumentDB

Como Aurora es para MySQL, DocumentDB para MongoDB (noSQL) crece automáticamente.

Amazon Neptune

Base de datos gráfica totalmente gestionada (grafos), redes sociales.

Amazon QLDB

Servicio sin servidor para base de datos de libros contables, se utiliza para uso de historial de cambios realizados en apps.

Amazon Managed Blockchain

Blockchain es tecnología para transferir dinero sin necesidad de una autoridad central.

El servicio crea red privada de blockchain.

AWS glue

Sin servidor, extrae información y transforma datos para analítica ETL.

DMS - Database Migration Service

Servicio para migrar de forma rápida y segura sin afectar la base de datos, heterogéneas y homogeneizar en motores

Otros Servicios

ECS (Elastic Container Service)

Lanzar contenedores de Docker en instancias EC2 y está integrado con el app load balancer

Fargate

También lanza contenedores de Docker pero serverless (sin EC2) solo con parámetro de CPU y RAM.

ECR (Elastic Container Registry)

Registro privado de Docker para almacenar tus propias imágenes de Docker para ejecutarlas después en ECS o Fargate.

Serverless => Los servidores siguen existiendo, pero ya no los gestionas (lambda).

Amazon EKS

Para mover tus contenedores de Docker basado en Kubernetes

Amazon Lambda (SERVERLESS)

Funciones virtuales, el escalado es totalmente automatizado y ejecución bajo demanda.

Precio por solicitud y tiempo de computación. Se monitoriza fácilmente por AWS CloudWatch. Soporta varios lenguajes backend.

- Pago por llamadas
- Pago por duración de cómputo

Con CloudWatch ves los logs de Lambda

Amazon API Gateway

El servicio como tal es serverless y escalable, y es usado para la creación y gestión de APIs

Amazon Web Services

Cloud Practitioner



AWS Batch (Por lotes)

Procesamiento por lotes totalmente gestionado a cualquier escala, (con un inicio y un final).

Lanza instancias EC2 adecuadas, los trabajos son imagenes de docker y se ejecutan en ECS. A diferencia de lambda no hay limite de tiempo, este si depende de EC2 y esta empaquetado como imagen de Docker.

AWS Lightsail (Para novatos)

Hace varias cosas, servidores, almacenamiento, bases de datos, y redes, ideales en que tengas poca experiencia en AWS.

Para apps sencillas, sitios web y test, no autoescala (precio por mes).

Servicios de Infraestructura

AWS CloudFormation

Forma declarativa para hacer una infraestructura de AWS, para evitar usar el dashboard, nada mas le dices que es lo que quieres, numero, de que servicio y ya (desde plantilla).

Declaras la infraestructura como codigo.

Aca facil levantas servicios y los tumbas facil, tambien ya hay plantillas de infraestructura

Puede declararse la infraestructura en un archivo .YAML o un JSON.

Stack Designer de CloudFormation

El sujeto se encarga de hacer el diagrama de la infraestructura de la nube.

AWS Cloud Development Kit (CDK)

Con un lenguaje de programacion ahora creas la infraestructura, como una lambda, pero esta cosa crea toda la estructura del Cloud.

Este codigo pasa por el CDK CLI para crear en base al codigo la plantilla de CloudFormation y crear la infraestructura del Cloud.

AWS Cloud Development Kit (CDK)

Con un lenguaje de programacion ahora creas la infraestructura, como una lambda, pero esta cosa crea toda la estructura del Cloud.

Este codigo pasa por el CDK CLI para crear en base al codigo la plantilla de CloudFormation y crear la infraestructura del Cloud.

Elastic Beanstalk (Paas)

Centrada para desarrolladores, donde todo esta concentrada en una sola vista, es gratuito pero pagas por lo que levantas de servicios.

- Configuraciones es gestionado por AWS
- Solo el codigo de la app es la que se supervia el desarrollador
- Puede usar LB + ASG automaticamente

Tiene soporte para muchos lenguajes de desarrollo. Tambien ves como estan EC2.

AWS CodeDeploy (desplegar auto)

Queremos desplegar nuestra app automaticamente, funciona con ec2, donde las intancias se van a actualizar y tambien funciona con tus servidores on-premise

AWS CodeCommit (GIT de AWS)

Antes de enviar el codigo de la app a prod, debe estar el codigo en un repositorio (como gitHub), CodeCommit es la competencia de GitHub. Facilita colaborar con otra gente.

AWS CodeBuild (Compilador)

Ejecuta y compila codigo fuente, serverless, es seguro, es un compilador y contruccion de codigo.

AWS CodePipeline (Orquestador)

Orquesta los pasos para que el codigo llegue a produccion.

Codigo -> Contruir-> Probar-> Aprovisionar -> Deploy

Basado en CI/CD (Integracion y entrega continua). Compatible con CodeCommit y esos servicios.



Amazon Web Services

Cloud Practitioner



AWS CodeArtifact (Dependencias)

Enfocado a las dependencias del código (gestión de artefactos), enfocado a administrar estos códigos de los que depende tu código. Funciona con herramientas como Maven, Gradle, NPM, Yarn, etc.

AWS CodeStart

Enfocado a gestionar de forma rápida todos los anteriores servicios, como codepipeline, EC2, beanstalk, codeDeploy, etc.

AWS Cloud9

Es un IDE en la nube, como un Netbeans y eso, es como un documento de drive y de que todos los miembros pueden modificarlo y verlo en tiempo real.

AWS System Manager SSM

Comandos a escala

Te ayuda a gestionar tus EC2 y On.Premises, es híbrido en AWS y te informa de el estado de tu infraestructura en servidores.

Es un agente SSM que se dedica a que puedas ejecutar código en todas las instancias a la vez. NO OCUPAS SSH.

AWS OpsWorks

Chef y Puppet te ayudan a realizar la configuración del servidor de forma automática, funciona EC2 o en On-Premise, alternativa a SSM.

¿Por que ser globales?

Edge Locations -> Puntos de presencia, donde AWS tiene sus servidores (puntos mas cercanos a los clientes).

Las razones son

- Latencia (Que los centros de datos esten cerca del cliente).
- Recuperar en desastres (Si pierdes en una zona tienes en otra).
- Es mas difícil de atacar.

Route 53 (DNS Dominios)

Es el servicio de AWS de DNS global y encamina a los usuarios a despliegues cercanos para menor latencia.

Políticas de Route 53

- Simple routing policy (Sin controles de salud).
- Distribución por peso: Para distribuir mas carga a instancias mas fuertes y menos a las mas debiles.
- Por latencia: Si esta mas lejos que no se conecte ahí, si no a la mas cercana
- Tolerancia a fallos: Si una instancia tiene un error no le enviara dicho trafico.

Cloudfront (CDN red global y cache)

Replica una parte de la aplicación en algun edge location o punto de presencia guardandolo en chace para optimizar y disminuir. **Muy util con archivos estaticos** como html, css, js o contenido multimedia.

Tambien protege a DDoS.

OAC => Origin Access Control

Amazon S3 Transfer Acceleration

Acelera las descargas globales de S3. Donde transfiere el objeto a un punto de presencia cercano al cliente para aumentar la velocidad y reducir la latencia.

AWS Global Accelerator (No cache)

Mejora la disponibilidad y rendimiento de aplicaciones globales usando la infraestructura global de AWS.

AWS Shield

Te protege ante ataques DDos

AWS Outposts

En cloud híbrido te permite que uses servicios de AWS en tus maquinas On-Premise, acceso de baja latencia y **migracion facil al cloud**.

AWS WaveLength

Lleva los servicios de AWS a el 5G, a maxima potenciaaaa, y con gran ancho de banda.

Integracion de Cloud

Sevicios para desacoplar

SQS
SNS
Kinesis

Amazon Web Services

Cloud Practitioner



Amazon SQS (Colas / desacoplar)

Permite desacoplar una aplicacion, es un servicio de mensajeria orientado a los microservicios y la comunicacion entre sistemas y se comunicuen de manera asincrona, pueden estar en la cola los mensajes hasta 4 dias.

Serverless

- Standard
- FIFO

Amazon Kinesis (Big Data tiempo real)

Servicio de recopilar, procesar y analizar datos de streaming en tiempo real.

- Streams: Ingerir datos a escalas de muchas fuentes
- Firehose: Cargar flujos de S3
- Analytics: Realiza analisis en tiempo real con SQL
- Video Streams: Para flujos de videos, analitica o machine learning

Amazon SNS (Desacoplar)

Distribuye todos los mensajes a los receptores, solo hay un publicador de mensajes pero puede haber muchos suscriptores.

Amazon MQ

Servicio gestionado de intermediacion / croker con rabbitMQ y activeMQ tambien para desacoplar pero sin ser gestionado totalmente por AWS.

Monitorizar el cloud

Amazon CloudWatch (Metrics)

Mide las metricas (variables) de como va el uso en el cloud (CPU, rendimiento, etc) y puedes verlo de forma grafica ese consumo cada n tiempo

- EC2 -> CPU
- Columen EBS -> Lectura / Escritura
- S3 -> Tamaño, read and write

Amazon CloudWatch Alarms

Para activar alarmas y enterarnos cada quehaya sucedido un evento en cloudwatch, por ejemplo, autoescalado, notificaciones SNS, Acciones EC2

Amazon CloudWatch Logs

Muestra los logs de eventos en la nube, como por ejemplo, (para EC2 hay que configurar si queremos ver los logs):

- Beanstalk (de aplicacion)
- ECS (De los contenedores)
- AWS Lambda (De funciones)
- CloudTrail en filtros
- Agentes de CloudWatch en EC2
- Router 53 (DNS)

EventBridge

Tienes posibilidad de configurar una configuracion en lambda o algo para realizar una accion cada evento que nosotros queremos, cada cierto tiempo.

Para programar acciones cada n tiempo

Algo detona el evento y tiene un destino final donde estara la consecuencia

CloudTrail (quien hizo que)

Servicio activado por defecto y obtiene un historial de eventos / llamadas a la API realizadas desde tu cuenta por

- SDC
- CLI
- Consola

Puede aplicarse a una o todas las regiones, si alguien borra un recurso checa el evento aqui, tambien sabras quien lo hizo!.

CodeGuru

Para hacer revisiones de codigo automatizadas (reviewer) (se integra chido con AWS Commit y GitHub) y sobre el rendimientos de las aplicaciones (profiler) (Si se esta matando buena CPU y detectar anomalia de la App).

AWS health dashboard

Muestra el historial de servicios y su salor en todas las regiones, mostrando informacion historica cada dia.

Por aqui se nos notifica si va a haber un evento por parte de Amazon que puede afectarnos (disponibilidad de los servicios).

Amazon Web Services

Cloud Practitioner



VPC (Redes en AWS)

IP elasticas

Permite que tu IP publica jamas cambia, ya que como vimos, al reiniciar un EC2 puede cambiar, con ip elastica no cambia, pero si te cobran este servicio.

VPC es la red de zona de disponibilidad que conecta todo tu AWS, por ejemplo para desplegar recursos. Y tambien se usan las tablas de enrutamiento.

Cada EC2 por ejemplo, tiene que pertenecer a la VPC y a una de sus subredes (red privada en AWS).

NACL

Es un firewall para la VPC, similar a un grupo de seguridad, pero con diferencia que NACL puede denegar el acceso de forma explicita, y esta administra toda la red, no solo la EC2. Tambien debe permitir el trafico de retorno.

VPC Peering

Nos permite comunicar dos VPC de forma primada para que ambas puedan comunicarse.

VPC Client

Nos permite comunicar desde nosotros como cliente en una red privada con las instancias y servicios de forma segura de AWS.

AWS Direct Connect (Hibrido)

Permite conectar tus instancias locales (On-Premise con las de AWS para tener un cloud hibrido pero bien conectado).

IAM Access Analyzer

Averigua que recursos de tu cuenta de AWS se estan compartiendo externamente

AWS Whitepapers (Guias)

Los AWS whitepapers son documentos detallados que explican diferentes conceptos, mejores prácticas y casos de uso relacionados con la computación en la nube y los servicios de Amazon Web Services (AWS).

Seguridad en AWS

AWS Shiel standard (contra DDoS)

Protege ante ataques DDoS a tus webs gratis

AWS Shiel advanced

Version mejorada y de pago de AWS shield standard

AWS WAF

Firewall para servicios web que filtra peticiones en base a reglas

AWS Network Firewall (VPC)

Firewall para proteger las VPC en AWS

Datos en reposo => S3

Datos en transito => Puede cifrarse

AWS KMS

Software de encriptacion de datos para un servicio en AWS

AWS Artifact

Acceso bajo demanda a descargar documentos de seguridad y conformidad de AWS y sus acuerdos

AWS GuardDuty

Descubrimiento con Machine Learning para detectar amenazas y proteger la cuenta de AWS, se alimenta de los logs.

AWS Config (Monitorear cuenta)

es un servicio de AWS que permite evaluar, auditar y monitorear la configuración de los recursos de AWS y sus normativas.

AWS Trusted Advisor (suggest)

Analiza y da recomendaciones a tu cuenta de AWS de rendimiento, costes, rendimiento, seguridad y tolerancia a fallos

- 7 core checks (developer y basico)(soporte para IAM, EBS, S3, MFA, RDS)
- Full checks (Casi todo, alarmas de limites de cloudwatch, AWS Support API)

IAM Access Analyzer

Averigua que recursos de tu cuenta de AWS se estan compartiendo externamente

Amazon Web Services

Cloud Practitioner



VPC (Redes en AWS)

AWS Pricing calculator

para que la empresa pueda comparar el coste de ejecutar su infraestructura de TI on-premise frente a AWS Cloud

AWS Macie

Machine Learning para datos sensibles