Mensajeria:

•(SNS) Amazon Simple Notification Service
→mensajes por tópico

•(SQS) Amazon Simple Queue Service
→almacena msj en la cola

•Lambda
→serverless
→una petición ejecuta el código
→solo cobra cuando se ejecuta

Responsabilidad compartida
•Cliente
→seguridad en la nube(virtual)

•AWS
→seguridad de la nube(fisico)

Caracteristicas:

usuario→persona(1 user a 1 persona)
politica→documento que permite el uso de servicios(JSON)
grupo→varios usuarios
rol→permiso temporal
(MFA) multi-factor auth→extra proteccion al login

Acceso de usuario:

•(IAM) identity and acces managment
→administra el acceso a servicios y recursos

•Aws Organizations
→ayuda a administrar cuentas en una ubicacion central(cuenta root) mediante scp.

•(SCP) Service Control Policies
→controla de forma centralizada los permisos de las cuentas de la organizacion.

Seguridad:

•(WAF) Aws Web Application firewall
→filtra a traves de reglas(https) capa 7

•Aws Shield→protege DDos

•Amazon Inspector
→evaluaciones de seguridad a nivel instancia
→entrega recomendaciones

•(KMS) Aws Key Managment Service
→Encripta con claves criptograficas

•Amazon GuardDuty
→Deteccion de amenazas a nivel red e instancias

•Minimo provilegio otorgado
→otorgar solo los privelegios necesarios para realizar la tarea especifica

Conformidad

•Aws Artifact
→repositorio de documentos de seguridad y conformidad firmados

•centro de conformidad
→mas info sobre conformidad

Monitoreo:
•Amazon CloudWatch
→Monitorea el uso y rendimiento y analiza metricas en un solo panel.

•Aws CloudTrail
→trackea y almacena toda la actividad de todo el sistema(que sucedio?, cuando ocurrio?, como?)

•Aws Trusted Advisor
→Ayuda en tiempo real recomendando mejores en base a pilares.

→optimizacion de costos
→seguridad
→tolerancia a errores
→rendimiento
→limites de servicio

Precio y soporte:

capa gratuita→siempre gratis
→12 meses gratis
→prueba de uso

capa pago→paga por uso
→pague menos al reservar
→pague menos con descuentos basados en volumenes

soporte basico→gratis documentos personal healthdashboard
→trusted advisor limitado

developer→buenas practicas(29usd/mes)

business →trusted advisor full(100usd/mes)

enterprice→posee director de cuentas (TAM) y da soporte(5500 usd/mes)

•(TAM) Technical Account Manager
→principal punto de contacto
→ofrece informacion orientacion, experiencia tecnica y practicas recomendadas

herramientas para pagos:

calculadora de precios
→estimaciones de costos

facturacion unificada
→recibe una sola factura para todas las cuentas de la organizacion.
→posee descuentos

•Aws Budget→establecer umbrales para el uso y costo.

•Aws Cost Explorer→viusualiza, comprende y administra costos.

•Aws MarketPlace→vender y comprar productos a terceros

Contenedores:

•(ECS) Amazon Elastic Container Service
→api simple
→Docker
→utiliza ec2

•(EKS) Amazon Elastic Kubernetes Service
→Kubernetes
→utiliza ec2

•AWS Fargate
→ejecuta ECS y EKS sin servidor
→NO usa ec2

Arquitectura:
•Monolitica
—1 solo bloque

•Microservicios
—mejor precio
—travel shoting

Networking:

•**(VPC)** Amazon Virtual Private Cloud
—establece areas privadas o publicas llamadas sub-redes

•Subred
—Seccion de la vpc en la que se colocan grupos de recursos aislados
—publicos o privados

publico—› internet gateway

privado—gateway privado virtual
—a traves de vpn(canal encriptado)

•Aws DirectConnect — enlace privado de fibra, la cual pasa por el proveedor de internet del cliente hasta la nube

Control/Seguridad:

•**(ACL)** Lista de control de acceso
—firewall virtual entre el gateway y la subred(dentro del vpc)
—›—permite todo el trafico de entrada y salida de forma predeterminada
—personalizado deniega todo
—**no posee estado**, por lo que revisa al entrar y salir

•Grupo de seguridad
—firewall virtual por cada instancia de ec2
—›—deniega el trafico entrante pero permite el trafico saliente de forma predeterminada
—**posee estado**, recuerda las conexiones y no checkea la salida.

Regiones:

•Region—Conjunto de zonas de disponibilidad(Availability zone)

•Zona de disponibilidad—varios centros de datos.

•Ubicación borde—almacena cache y algunos servicios

•**Seleccion de región:**
—requisito legales
—proximidad al cliente
—servicios disponibles
—precio

(POP)Punto de presencia:

•Amazon CloudFront
—servicio global de entrega de datos
—almacena cache estatico
—utiliza la ubicacion borde

•aws Outposts
—lleva un rack a la instalacion
—extiende la infrasestructura de aws a el centro de datos en la instalacion

Interaccion:
•Consola de administracion—dashboard
•Interfaz de la linea de comandos—cmd/powershell
•kit de desarrollo (SDK)

Elastic Cloud Compute (EC2)

Escalados:

•Auto-scaling
—dinamico y predictivo
—elimina y agrega instancias

•**(ELB)** Elastic Load Balancing
—balancea la capacidad
—distribuye el trafico automatico
—1 punto de contacto para el auto-scaling

Precios:

•Bajo demanda
—Inmediato.

•Spot
—› oferta/demanda
—resiste interrupciones

•Bajo reserva
—compromiso 1-3 años

•Instancia dedicada
—instancia única para el cliente con vpc

•Host dedicado
—servidor fisico único para el cliente

Tipos:

•General

•Optimizado para computación.
—› + cpu

•Optiimizado para memoria
—› + ram

•Informatica acelerada
—› + gpu

•Optimizada para almacenamiento
—› + iop's (mejores ssd)

Interaccion con la red global:

•**(DNS)**Sistema de nombres de dominio
→traduce las ip a nombre y de nombre a ip

•Route 53—dns de amazon
—registra nombres de dominio
—chekea la salud de destino y redirecciona a otra region si hay problemas

Migrar a la nube:

(CAF) Aws Cloud Adoption Framework
(marco de adopcion de la nube aws)
→da asesoramiento a la empresa para migrar de forma rapido y fluido

•6 perspectivas

de negocio
→business
→personas
→gobernanza

tecnicas
→plataforma
→seguridad
→operaciones

•estrategias(6 R)
→re-hospedar
→re-aprovisionar la plataforma
→rediseñar o refactorizar
→re-adquirir
→retener
→retirar

Familia de Aws Snow:
—llevar datos a la nube de manera offline

•Aws SnowCone(8 tb)
→dispositivo como un disco duro grande.

•Aws Snowball Devices
→optimizado para computo y almacenamiento. es como un disco muy grande(maleta de avion)

•Aws Snowmobile(100 pb)
→es un camion
→datos a escala de exabytes.
→solo disponibles en regiones de aws

Innovacion:

•Aws Well Arquitected Framework
—ayuda a entender como diseñar y operar con buenas practicas

6 pilares:

→Excelencia operativa
→seguridad
→fiabilidad
→eficacioa del rendimiento
→optimizacion de costos
→sustentabilidad

Almacenamiento:

En bloques:
—particiona archivos en bloques de igual tamaño y se usa para ec2
•Almacen de instancia
—se borra todo cuando se termina la instancia

•**(EBS)** volumenes de amazon
→se almacena en una zona de disponibilidad
→la data se mantiene cuando se termina la instancia
→es elastico

•EBS Snapshot
→copia de seguridad a datos, solo a los cambios, el resto se mantiene almacenado para no duplicar.

De objetos:
—cualquier tipo de archivo(jpg,mp4,etc)
—no se puede editar, se cambia el archivo entero.

•**(S3)** Amazon Simple Storage Service
→buckets, almacenado regionalmente pero con nombre unico global
—se replica en hasta 3 zonas y maximo 5 teras

Tipos:

s3 standar
—3 zonas de disp

s3 standar poco frecuente
→giga mas barato que el anterior pero recuperacion mas cara

s3 zona unica
→se almacena en 1 zona

s3 intelligen tiering
→coste de monitorieo y se determina el mismo el tipo de almacenamiento

s3 glacier
—recupera datos en minutos o horas

s3 deep archive
—recupera los datos en 12hrs

De archivo:
—brinda sistema de archivos compartidos entre diferentes usuarios

•**(EFS)** Amazon Elastic File Sistem
→serverless
→guarda datos en varias zonas de disp
→linux

—la opcion para windows es (FFX)

Base de datos:

•Relacional
•**(RDS)** Amazon Relational Database Service
→estructurado, escala y opera db
→automatiza tareas y es seguro
—Aurora→reduce costo, 6 copias en 3 zonas

•No-relacional
—clave-valor
→mas rapido
—DynamoDb→serverless auto escalable bajo demanda

(DMS) Database Migration Service
→migra de sql a no sql y de db fuera de la nube a la nube y al reves.

Otras:
Redshift— bigdata/datawarehouse
DocumentDb—documentos mongodb
Neptune—datos altamente conectados
QLDB—inmutable y segura
Manage blockchain—blockchain crypto
Elastic cache—cache para optimizar lectura
Dynamo Acelerator—de milisegundo a micro segundo